A Graphical Password Authentication System

Ahmad Almulhem
Computer Engineering Department
King Fahd University of Petroleum and Minerals
Dhahran, Saudi Arabia
ahmadsm@kfupm.edu.sa

Abstract

Graphical passwords provide a promising alternative to traditional alphanumeric passwords. They are attractive since people usually remember pictures better than words. In this extended abstract, we propose a simple graphical password authentication system. We describe its operation with some examples, and highlight important aspects of the system.

1 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, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use.

Alphanumerical 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 alphanumerical 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.

2 Graphical Passwords

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.

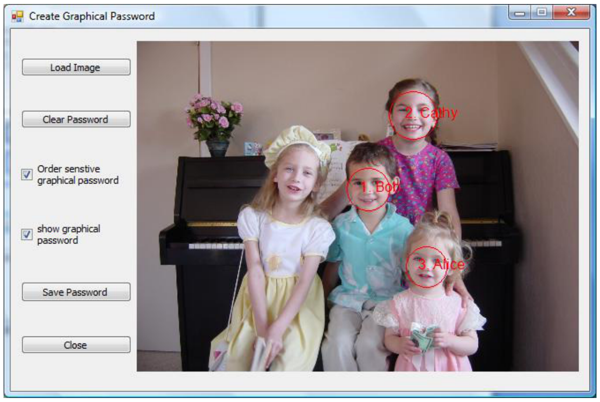
In general, graphical passwords techniques are classified into two main categories: recognition-based and recall-based graphical techniques [7]. In recognition-based techniques, a user is authenticated by challenging him/her to identify one or more images he or she chooses during the registration stage. 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].

3 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.

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.



☑ Order senstive graphical password

☑ show graphical password

1. Bob

2. Cathy

3. Alice

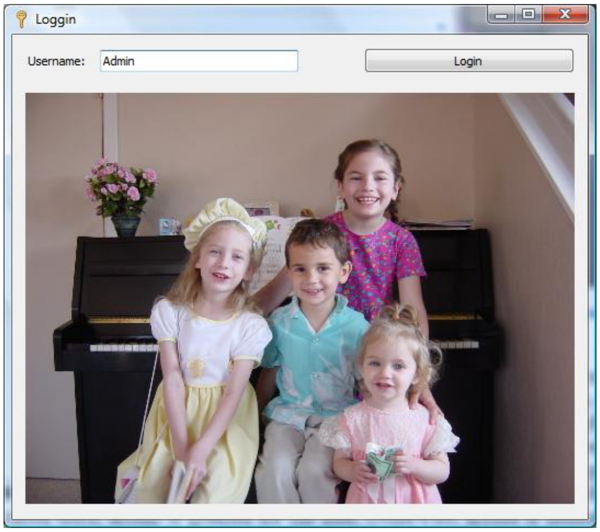
Figure 1. An example of creating a graphical password using the proposed system.

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 2, we show an example of the login screen.

4 Implementation and Discussion

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

- LoginInfo: Contains username, graphical password, and related methods.
- GraphicalPassword: Contains graphical password information and related methods.
- SelReg: Contains fields about selected regions (POIs).



Username: Admin

Figure 2. Login Screen

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.

5 Conclusion

User authentication is a fundamental component in most computer security contexts. In this extended abstract, we proposed a simple graphical password authentication system. The system combines graphical and text-based passwords trying to achieve the best of both worlds. It also provides multi-factor authentication in a friendly intuitive system. We described the system operation with some examples, and highlighted important aspects of the system.

6 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.