Graphical Password

Siddharth Singh[1] Vaishnavi Sawant[2] Alisha Shah[3] Pratik Prasad[4]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Thakur Polytechnic, Mumbai, India

Abstract— The most common authentication method of computer is to use alphanumerical usernames and passwords. Graphical password provides a promising alternative to alphanumeric passwords. Graphical password is attractive since it become easy for people to remember pictures better than words. In this abstract, we recommend a simple graphical password authentication system. This method has been shown to have significant drawbacks. For example users chooses password that is easy to remember. On the other side if a password is hard to guess, then it is often difficult to remember. To solve this issue, researchers have developed authentication methods that use pictures as password.

Key words: Graphical Password, Graphical User Interface (GUI), Authentication, Password Images, OTP (One time password)

I. INTRODUCTION

A graphical password is a secured system that work by having the user's select from pictures provided to select from, in a specific order, presented in a graphical user interface. Therefore for this reason, the graphical-password approach is mostly called as graphical user authentication (GUA).A graphical password is easier than a text based password for people to remember. Consider an eight-character password is required to gain entry into a particular computer network server. Instead of w8KiJndj, for example, a user might select images of the moon (from among a screen full of real and fictitious stars), the country of Canada (from a map of the world), etc. Graphical password may provide better security than text-based password because many people in an attemptremember text based password rather they refer plain words (rather than the suggested jumbling characters and symbols). A dictionary search can often hit on a password and give an easy access to a hacker to gain entry into a system in very few seconds. Suppose a series of selective images is used on successive screen frames, and if there are many pictures on each frame, a hacker willtry every possible combination at random. If there are 100 pictures on each of the eight-frames in an 8 picture password, there are (1008), or (10) quadrillion (10,000,000,000,000,000) combination that can form the graphical password pictures. If the system could built in delay of only 0.2 second following the selection of each picture until the presentation of the next frame, it would take millions of years long to break into the system by hitting it with random picture sequences.

II. GRAPHICAL PASSWORD

Graphical passwords were originally introduced by Greg Blonder (1996). In this concept, we recommend to use a Graphical Password to Login into a System instead of a simple Text based Password. In statics, it is shown that Graphical Password is difficult to crack for hackers.

In this concept, a picture would appear on the screen, and then the user will click on a few chosen regions. If the correct regions are clicked in, then the user would be authenticated. Graphical passwords refer to using pictures as password. In theory, graphical passwords can be easily remembered, since humans remember pictures better than words. Also, they should be able to resistant attacks like brute force, shoulder surfing n piggy backing since the search space is practically infinite. In general, graphical password techniques are classified into two categories: recognition based and recall-based graphical techniques. In recognition-based techniques, a user is presented with the set of pictures and the user passes the authentication by recognizing and identifying the pictures he selected during the registration stage. In recall-based techniques, a user is asked to clone something that he created or selected earlier during the registration stage. Pass-faces is a recognition-based technique, where authentication of user is done by challenging him/her into recognizing human faces. Earlier recall based graphical password authentication approach was discovered by Greg Blonder. In this approach, an user create a password by clicking on several regions on an pictures. During authentication, the user may click on those locations. Pass-Points had built on Blonder idea, and it over comes on some of the limitations of his concept.

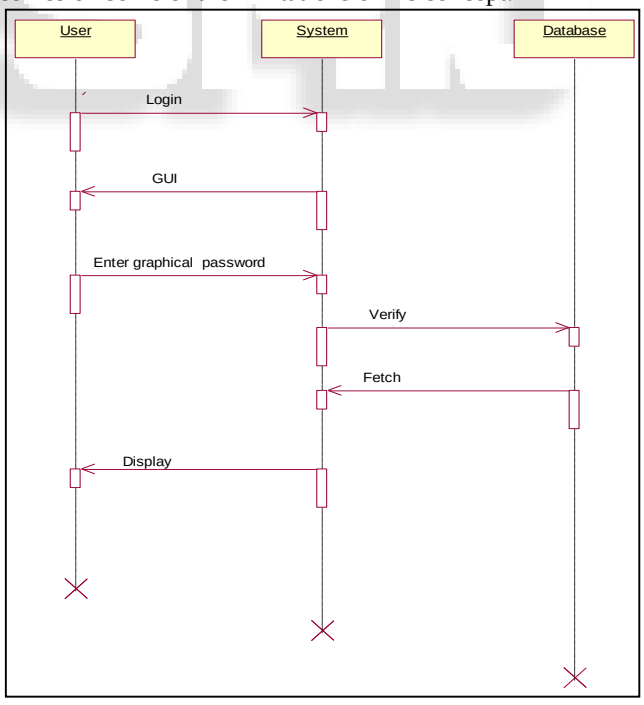

Fig. 1: Sequence Access System

III. PROPOSED SYSTEM

At the time of registration, a user creates a graphical password by first selecting 8 pictures from set of 25*8 pictures he or she chooses. The user will be authenticated if right pictures are selected from presented 25*8 set of

pictures. If wrong sequences of the pictures are selected then user won't be authenticated and "Wrong Password" message will be displayed. If 3 consecutive wrong attempts are made then system will shut down itself. In case user(admin) forgets the password, then an auto OTP(one time password)is generated which is send as an email to the user using which user can verify themselves and can set the new password.

Fig. 2: Login Page

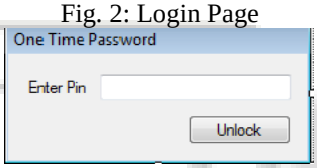

Fig. 3: OTP (One Time Password)

IV. Implementation and Discussion

A. Usability

Main reason for graphical passwords is that pictures are easier to remember but text strings are difficult to remember. A complaint among the users is that log-in process and the password registration take too much time, usually in recognition-based approaches.

B. Reliability

Major design problem for recall-based methods is the reliability and accuracy of user input recognition. Usually in this concept, the error tolerance have to be set carefully - overly high toleration may lead to many false positives, while overly low tolerances may lead to many false negatives.

C. Brute Force

Very few researches has been done to study the difficulty of cracking graphical passwords, Because graphical passwords are not used in practices, there is no other way on real cases of breaking graphical passwords. In brute force it is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs automatically needed to generate accurate mouse motion to follow human input, which is particularly difficult for recall based graphical passwords.

D. Dictionary Attacks

Since Dictionary attacks recognition based graphical passwords include input of mouse instead of input of keyboard, it will be difficult to carry out dictionary attacks against this type of graphical passwords.

E. Spyware

Except few exceptions, logging of key or key listening spyware cannot be used to break graphical passwords. Whether "mouse tracking" spyware will be an effective tool against graphical passwords is not clear.

Overall, it is tough to break graphical passwords using the attacks like brute-force, search dictionary attack, and spyware. There is a need for more in-depth research that investigates possible attack methods against graphical passwords.

V. Do and Dont's

- Use easy to remember picture but hard to crack.
- Avoid hotspots on the picture while selecting click point.
- Always remember the click point and the picture which will become helpful for knowledge based authentication.
- Choose minimum 3 pictures or maximum 5 pictures for this password system.
- As no of pictures increases the password becomes that tight.
- Do not use more bright and black pictures for password.

VI. Advantages

- Graphical password schemes provide a way of making more human friendly passwords.
- Here the security of the system is very high.
- Dictionary attacks are feasible.
- An average, millions of years to break into the system.

VII. Conclusion

User authentication is a fundamental component in almost every computer security contexts. In this abstract, we recommend a simple graphical password authentication system. The system combines both graphical passwords and text based passwords in order to achieve the best of both the worlds. In this abstract we conducted the system operation with some examples, and highlighted important aspects of the system. It also provides multi factor authentication in a friendly intuitive system. Statics suggest that it is more difficult to break graphical passwords using the traditional attack like brute-force, search dictionary attack, or spyware. More research and user study are needed for graphical password techniques to achieve higher levels of ability and usefulness.

References

[1] Jansen, W. Gavrila, S. Korolev, V. Ayers, R. Swanstrom,"Picture Password: A Visual Login Technique for Mobile Devices", NISTt NISTIR 7030, 2003
[2] Real User Corporation, Passfaces TM http://www.realuser.com, Accessed on January 2007.
[3] Blonder, G.E. (1996). Graphical Passwords.United

States Patent 5559961.
[4] Birget, J.C., Hong, D., and Memon, N. (2003). Robust discretization, with an application to graphical passwords.
[5] D. Hong, S. Man, B. Hawes, and M. Mathews, "A passwordscheme strongly resistant to spyware", In Proceedings ofInternational conference on security and management, LasVergas, NV, 2004.
[6] R. Dhamija and A. Perrig. "Déjà vu: A User Study UsingImages for Authentication", In Proceedings of the USENIXSecurity Symposium, 2000.
[7] Wiedenbeck, S., Waters, J., Birget, J.C., Broditskiy, A., & Memon, N. (2005). PassPoints: Design and evaluation ofa graphical password system.
[8] G. Blonder, "Graphical Password", In Lucent Technologies, Inc., Murray Hill, NJ,United States Patent 5559961, 1996.
[9] SFR IT-Engineering, http://www.sfrsoftware.de/cms/EN/pocketpc/viskey/,Accessed on January2007

