Graphical Password Authentication Scheme through Encryption

Abhishek Bhardwaj[1]
M.Tech*, CS
Sobhasaria Engineering College, Sikar

Ashwani Garg[2]
Assistant Prof., CSE Dept.
Sobhasaria Engineering College, Sikar

Deepika Gupta[3]
Assistant Prof., CSE Dept.
Marudhar Engineering College, Raisar

Abstract

Password in authentication system is supporting users for reliable communication. A system which is providing the secured communication pathways across a unsecured network without lacking the security at any level. So researcher goes for graphical environment for generating the password. Graphical password system uses the graphics, images for generating the password. There are various virtual and graphical environments present in the market but mostly are still immature because they are not providing the security with already created password. Therefore, this project merges a graphical environment for generation of password. Using a graphical password, users click on images rather than type alphanumeric characters. Here this password is again encrypted for providing double security. Attacks like bruteforce attack and dictionary attack, keylogger attack can be successfully abolishing using this method.

Introduction

Security concerns are dramatically increased due to increase of computer usage. One major security concern is authentication, which is the process to validate a user to get enter into a system. It is the process of validating who you are to whom you claimed to be. Graphical passwords can be divided into two categories as follows: a) Recognition based and b) Recall based .Various graphical password schemes have been proposed now a days. The idea behind the Graphical passwords is that the users can recall and recognize pictures better than words. However, a long period of time is required for some of the graphical password schemes to be performed. Moreover, most of the graphical passwords can be easily observed or recorded while the legitimate user is performing the graphical password; thus, it is vulnerable to shoulder surfing attacks. Currently, most graphical passwords are still in their research phase and require more enhancements and usability studies to deploy them in the market.

The main difficulty in designing secure password mechanisms arises from the fact that password space is usually small and much easier to attack than random cryptographic keys. Moreover, when using

passwords as cryptographic keys, we make the assumption that the cryptographic functions remain secure even when the keys are chosen from a very small set. These assumptions are so unusual that, to the best of our knowledge, no one has been able to formally define the requirements from these cryptographic functions under which existing protocols can be proved secure. The problem arises because passwords are expected to comply with two fundamentally conflicting requirements:

1) Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.

2) Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text

3) It should provides secrets that can be easily revoked or changed.

Related Work

Graphical passwords were originally described by Blonder. In this scheme image would appear on the screen, and the user would click on a few chosen regions of it. If the correct regions were clicked in, the user would be authenticated. Memory of passwords and efficiency of their input are two key human factors criteria. Memorability has two aspects: (1) how the user chooses and encodes the password and (2) what task the user does when later retrieving the password. In a graphical password system, a user needs to choose memorable locations in an image. Choosing memorable locations depends on the nature of the image itself and the specific sequence of click locations. To support memorability, images should have semantically meaningful content because meaning for arbitrary things is poor. This suggests that jumbled or abstract images will be less memorable than concrete, real-world scenes. Depending on the graphical password system, at retrieval time users will be presented with either a recognition task or a cued recall task. In a graphical password system based on recognition, the user has to be able only to recognize previously seen images, making a binary choice of whether the image is known or not known. Recognition is an easier memory task than pure, unaided recall. In our password system we use an intermediary form of recollection between pure recall and recognition, cued recall. Scanning an image to find previously chosen locations in it is cued recall because viewing the image reminds, or cues, users about their click areas. In this new project If user is sitting in a Lan of o big organization than if there secure communication with one another is required than this technique help a lot.

Conclusion and Future Work

Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack, or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood.

It can be extended as a person identification program for computer security and internet services. To be differentiated from the traditional authentication method,

which typically requires a user name and a password (text, graphical, finger prints. etc) and authenticates the user right away, our program may allow the user to do their daily activities based on their will, and then identifies the user based on the comparison between their activity and the predicted activity.

Adding more users' biometric parameters and factors into the registration process would certainly be an improvement, examples such as: recording the users' typing patter alone with the mouse motion, or the eye fixation during different activities. Nevertheless, biometrics as an authentication technique is still at its very early stage, there is still much more work to do.

References

[1] M. N. Doja and Naveen Kumar, "Virtual Password: Virtual environment based user authentication", 2007.

[2] Gauri Rao, Dr. S.H. Patil, "Three Dimensional Virtual Environment for Secured and Reliable Authentication", Journal of Engineering Research and Studies E-ISSN 0976-7916, June 2011.

[3] Xiaoyuan Suo, Ying Zhu, G. Scott. Owen, "Graphical Passwords: A Survey", in Proc. 21st Annu. Computer Security Appl. Conf., pp. 463–472, Dec. 5–9, 2005.

[4] Duhan Pooja, Gupta Shilpi , Sangwan Sujata, & Gulati Vinita, "Secured Authentication: 3d Password", International Journal of Engineering and management Science, VOL.3(2) 2012: 242 - 245 ISSN 2229-600X, 2012.

[5] T.Sujanavan, Dasika Ratna Deepthi, "A More Secure Authentication through A Simple Virtual Environment", International Journal for Advances in Computer Science, ISSN - 2218-6638 on March 2011.