A Novel Security Model for Password Stealing and Password Reuse Attacks

P. Kasthuri[1], R. Kokila[2]

[1, 2]University College of Engineering, BIT Campus, Trichy, India

Abstract: ***The aim of the project is to design a user authentication protocol named Opass which leverages a user cell phone and short message service to password stealing and password reuse attacks. Opass only requires a unique phone number, and involves a telecommunication service provider in registration and recovery phase. This protocol is generated a new password when a user enter the webpage anytime. The generate password is transfer to particular mobile. This Opass system used HMAC (Hash Message Authentication Code) algorithm. The password the user can use the webpage successfully. Through Opass, users only need to remember a long-term password for login on all websites.***

Keywords: Network security, password reuse attack, password stealing attack, user authentication.

1. Introduction

A Computer Network is an interconnected group of autonomous computing nodes which use a well- defined, mutually-agreed set of rules and conventions known as Protocols, interact with one another meaningfully and allow resource sharing preference in a predictable and controllable manner. Study of methods of analysis of security requirements and needs of such system and consequent design, implementation and deployment is the primary scope of the discipline named as Network Security. Although named as network security, the principles and mechanisms involved herein do apply to internetwork as well.

2. Related Works

In 2004, Blake Ives, Kenneth R. Walsh and Helmut Schneider concluded that using same password across various websites causes domino effect. In domino effect, when a weak system losses its password, some information will be revealed that will aid the hackers in infiltrating other systems which may cause loss of huge data [1].

Shirley Gaw and Edward W. Felten studied online accounts and password management strategies for that accounts. y did not help for recalling password of an online account but their tips to strengthen passwords but failed to explain the nature of dictionary attacks [2].Because of such different drawbacks of text passwords graphical passwords were introduced years before.

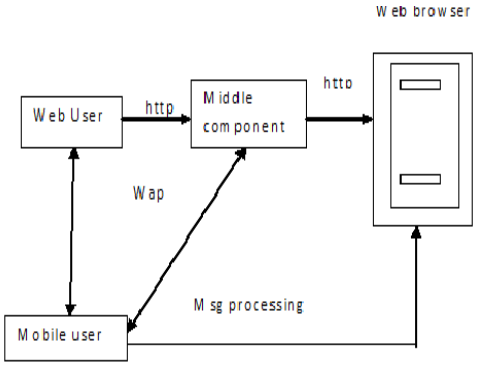
Ian Jermyn, Alain Mayer, Fabian Manrose, Michael K. Reiter and Aviel D. Rubin evaluated new graphical password schemes to achieve better security than text passwords. When Graphical password users were creating passwords they were able to quickly and easily create a valid password, but to learn those passwords they had more difficulty than alphanumeric password users. However, the graphical users took longer time and made more invalid password as compared to alphanumeric users while practicing their passwords [3].

Sonia Chiasson, Alain Forget, Elizabeth Stobert, P.C. van Oorschot, Robert Biddle studied Multiple Password Interference and Click-Based Graphical Passwords. They concluded that graphical password users managed significantly better than text password users and they did not use similar passwords across multiple accounts. They also concluded that remembering multiple click-based graphical passwords is easier than remembering multiple text passwords. Text password users made comparatively more recall errors than graphical password users [4].

In 2005 researcher's Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy and NasiMemon introduced the concept of graphical password system called Pass Points which was based on two areas i.e. security and usability[5].

3. Proposed System

I design a user authentication protocol named oPass which leverages a user's cell phone and short message service to plan password stealing and password reuse attacks. OPass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through oPass, users only need to remember a long-term password for login on all websites. After evaluating the oPass prototype, we believe oPass is efficient and affordable compared with the conventional web authentication mechanisms. This long-term password is used to generate a chain of one-time passwords for further logins on the target server. Then, the program automatically sends a registration SMS message to the server for completing the registration procedure. The confidentiality and integrity algorithms are f8 and f9, respectively. Algorithm f8 and f9 are based on a block cipher named KASUMI where f8 is a synchronous binary stream cipher and f9 is a MAC algorithm. The user name is the only information input to the browser. Next, the user opens the oPass program on her phone and enters the long-term password, the program will generate a one-time password and send a login SMS securely to the server. The login SMS is encrypted by the one-time password.



System Architecture

4. Simulation Testbed

The proposed system is implemented in .Net frame work. C# is used for front-end designed. For maintaining information MySQL database is used. Sample screen shots are given below.

Figure 1: The login to the Opass applications

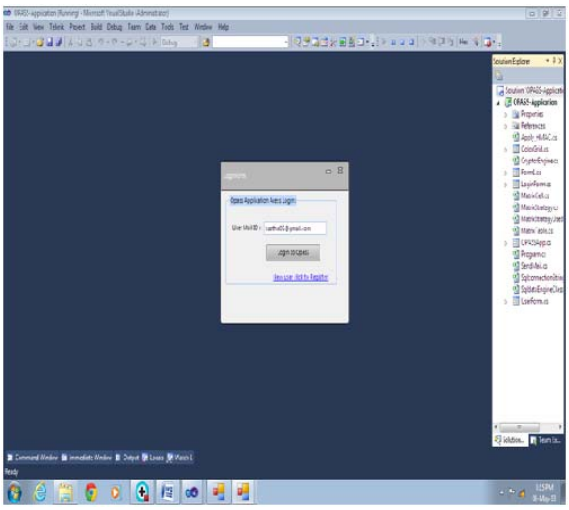


Figure 2: Opass application security process to login process

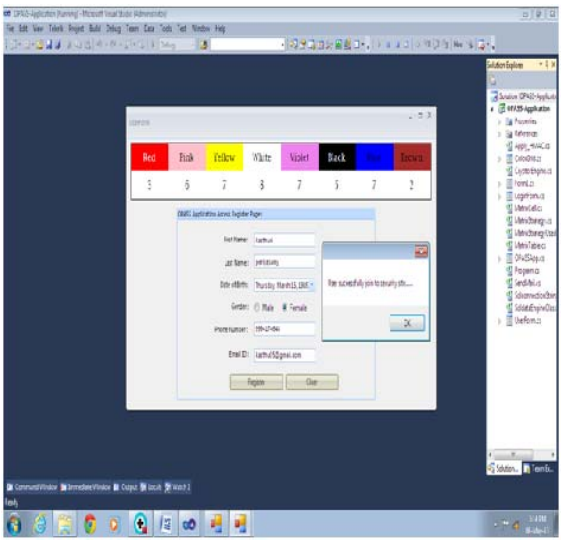
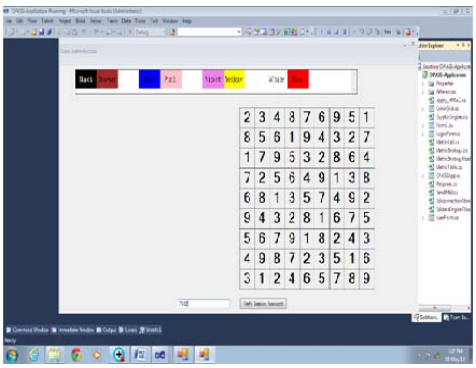


Figure 3: Verify the session password and then enter to opass applications



5. Conclusion

In this paper implementing opass is a user authentication protocol. Opass which leverages cell phone and SMS to thward password stealing and password reuse attacks. The design of opass is to eliminate the negative influence of human factors as much as possible. Though opass system each user only needs to remember a long-term password which has been used to produced her mobile. Users are free from typing any password into untrusted computer for login all websites compared with previous schemes, opass is the first user authentication protocol and password reuse attacks simultaneously. The reason is opass adopts the one-time password approach to ensure independence login. So conclude that opass is more secure than the original login system

References

[1] B. Ives, K. R. Walsh, and H. Schneider, “The domino effect of password reuse,” Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.

[2] S. Gawand E. W. Felten, “Password management strategies for online accounts,” in SOUPS ’06: Proc. 2nd Symp. Usable Privacy. Security, New York, 2006, pp. 44–55, ACM.

[3] D. Florencio and C. Herley, “A large-scale study of web password habits,” in WWW ’07: Proc. 16th Int. Conf. World Wide Web., NewYork, 2007, pp. 657–666, ACM.

[4] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, “Multiple password interference in text passwords and click-base graphical passwords,” in CCS ’09: Proc. 16th ACM Conf. Computer Communications Security, New York, 2009, pp. 500–511, ACM.

[5] Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, “Thedesign and analysis of graphical passwords,” in SSYM’99: Proc. 8thConf. USENIX Security Symp., Berkeley, CA, 1999, pp. 1–1, USENIX Association.

[6] Perrig and D. Song, “Hash visualization: A new technique to improve real-world security,” in Proc. Int. Workshop Cryptographic Techniques E-Commerce, Citeseer, 1999, pp. 131–138.

[7] J. Thorpe and P. van Oorschot, “Towards secure design

choices for implementing graphical passwords," presented at the 20th. Annu. Computer Security Applicat. Conf., 2004.
[8] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," Int. J. Human-Computer Studies, vol. 63, no.12, pp.102–127, 2005.
[9] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in AVI '06: Proc. Working Conf. Advanced Visual Interfaces, New York, 2006, pp. 177–184, ACM.
[10] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in CCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170, ACM.

Author Profile

P. Kasthuri received the B. Sc Computer Science in Cauvery College for Women Trichy and MCA degree in University college of Engineering, BIT-Campus, Trichy.