www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 3 March, 2014 Page No. 5206-5209

Comparison on Various User Authentication Protocols Against Password Stealing And Reuse Attacks

Aparna CM, Binisha Mohan, Alpha Vijayan

[1]MBC College of Engineering and Technology, Computer Science and Engineering,
Mahatma Gandhi University, Kerala, India
aparnasajee@gmail.com

[2]MBC College of Engineering and Technology, Computer Science and Engineering,
Mahatma Gandhi University, Kerala, India
binisham36@gmail.com

[3]MBC College of Engineering and Technology, Computer Science and Engineering,
Mahatma Gandhi University, Kerala, India
alphavijayan@gmail.com

Abstract: ***Nowadays passwords are really an influential tool to keep all data and information digitally safe and secure. Text password are most popular compared with other formats of passwords, since information that resides in text passwords are more simple and convenient. However, text passwords are more prone to be stolen and are not always strong enough and come across different vulnerabilities. If the person creates a weak password or a password that is reused in many other sites, the intruders can easily get it. If the password is stolen ,it can be used for all the websites and this is what is called the Domino Effect. One of the risky environment is when a person enters his/her password in a computer that is not trust-worthy the password is prone to attacks like malware, phishing and key loggers etc. In this paper, a user authentication protocol is designed, which leverages a user's cell phone and short message service to thwart password stealing attacks .The protocols requires a unique phone number that will be possessed by each participating website. A telecommunication service provider is involved in the registration and the recovery phases. The main concept of the paper is reducing the password reuse attack and password reuse attacks. The one time password technology reduces the password validity time. The good performance had improved the security.***

Keywords: One-Time Password, Hash Function, Network Security, Password Reuse Attack

1. INTRODUCTION

To log into the website successfully, users must recall their passwords. Generally, password based user authentication can resist phishing and brute force attacks if strong passwords are selected by users. But, password-based user authentication has got a major problem that humans are not experts in memorizing text strings. Thus, most users would choose weak passwords (i.e., easy –to-remember passwords) even if they know that weak passwords might be unsafe. Another main problem is that users tend to reuse passwords across various websites. Password reuse may cause users to lose their sensitive information stored in different websites if an external agent hacks one of their passwords. This attack is referred as password reuse attack. The above problems mentioned are mainly caused by the negative influence of human factors. Therefore, it is more important to take the human factors into consideration while designing a user authentication protocol. Since humans are more sharp in remembering graphical passwords than text passwords many graphical password schemes[1] were designed. Password management tools automatically generate the strong passwords for each website, which helps to ride password reuse problems. The main advantage is that users only have to remember a master password to access the password management tool. Despite with the assistance of these two technologies—graphical password and password management tool—the user authentication system still suffers from some drawbacks. Although graphical password[2] is a good idea, it is still vulnerable to various attacks and is not yet mature enough to be widely implemented in practice .Password management tools work well; however, general users doubt about its security and thus feel uncomfortable about using it. Also, the lack of security knowledge is another great trouble. The effects of password stealing attacks should also be considered along with password stealing and reuse attacks. Many studies have proposed various schemes to defend against password stealing attacks and password reuse attacks. To provide more reliable user authentication some researches focus on three-factor authentication rather than password-based authentication. The three-factor authentication deals with what you have (e.g., token),what you know (e.g., password) and who you are (e.g., biometric).Even if three-factor authentication is a comprehensive defence mechanism against password stealing attacks, it requires comparative high cost. Thus, the two-factor authentication is more attractive and practical than that of three-factor authentication. Many banks support two-factor authentication, but it still suffers from the negative influence of human factors, like the password reuse attack. Users should memorize another four-digit PIN code to work together with the token.

A user authentication protocol which leverages a user’s cell phone and short message service (SMS) helps to prevent password stealing and password reuse attacks.

The main reason for stealing password attacks is that users type passwords to untrusted public computers. Therefore, the main concept is to free users from having to remember or type any passwords into the computers for authentication. Unlike generic user authentication[3], a new communication channel, SMS,is used to transmit the authentication messages .A new component called the cell phone is used to generate one-time passwords is being used.

1.1 ARCHITECTURE OF USER AUTHENTICATION PROTOCOL AND ITS ASSUMPTIONS

Figure 1 describes about the environment (and architecture) of the user authentication protocol system. For users to perform secure login on a conventional computer (kiosk), user authentication protocol mainly consists of a trusted cell phone, a browser on the kiosk, and a web server that users wish to access. The user operates his/her cell phone and the conventional computer directly to accomplish the secure logins in to the web server.

The communication between the cell phone and the web server is done with the help of the SMS channel. The web browser interacts with web server with the help of the internet. In the protocol design, the cell phone interact directly with the kiosk. The general approach is mainly to select available interfaces on the cell phone, Wi-Fi or Bluetooth.

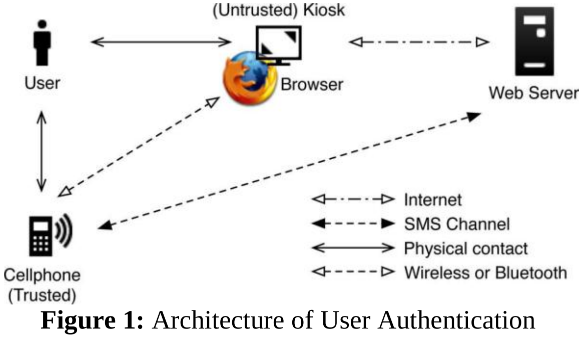

Figure 1: Architecture of User Authentication Protocol

2. RELATED WORKS

2. 1: PASSWORD MANAGEMENT STRATEGIES FOR ONLINE ACCOUNTS

As there is widespread use of password authentication in online correspondence, shopping and subscription services, there is growing concern about identity theft. When people use their same passwords across multiple accounts, vulnerability is increased to large extent and reusing same password can help an attacker take over several accounts. From the study obtained, the majority of users have weak passwords and had three or fewer passwords which were reused twice. Furthermore, over time, people accumulated more accounts but did not create more passwords which increase the rate of password reuse attacks. They sometimes fail to realize that personalized passwords such as phone numbers can be cracked. Here they discuss about how the current systems support poor password practices and also present potential changes in website authentication systems and password manager.

The main limitation in password management is that the average user can't and won't even try to remember complex enough passwords to prevent phishing and other dictionary attacks. When users are asked to choose a complex password they choose easy to remember password which leads to password stealing. The password study also focuses on online accounts. Website authentication scales up a user's password management problem.Hash Visualisation [4] is also another method against password stealing. For real world interactions, users can leverage physical context: Second, real world interactions also have more regularity: Here they present a survey of how users manage passwords for online accounts. With this background on what users do, they can develop supportive technologies for password management. The questionnaire on password management strategies also demonstrated that people relied on their memory. Based on study it shows that the users are not aware of the problem of password reuse attacks. Even though people have access to a computer and the internet when logging into online accounts, they were able to show the technology they used did not help them with recalling their passwords..Users need to be aware of the problems due to use of same password in different websites. Furthermore, they demonstrated that password reuse is likely to become more problematic over time as people accumulate more accounts and having more accounts implies more password reuse.

2.2: PASSPET: CONVIENIENT PASSWORD MANAGEMENT AND PHISHING PROTECTION

Passpet is a tool that improves both convenience and security of website logins through combination of techniques. Password hashing method helps users manage multiple accounts by converting a single password into a different password for each account. In this case the user need to remember only one password. Password-strengthening defend dictionary attacks. Modify the user interface defends against user-interface spoofing attacks. They make new improvements to these techniques, discuss how they integrated into one tool and compare Passpet to related solutions for manage passwords and prevent phishing.

Passwords are the widely used authentication on the Web, but it has many usability problems and security weaknesses. Security of password depends on choosing password that is unique and hard to guess, long passwords are very difficult to remember and retype correctly. The passwords that are easiest memorize tend to be vulnerable to dictionary attacks, in which an attacker tries to guess password by constructing possibilities from some lists of words and common passwords. Frequently changing the password helps to resist attack, but it make memorizing passwords become a harder task. Using same password or related password at multiple sites reduces password secrecy, memorizing different passwords for every site imposes burden on human users. Password login forms also vulnerable to phishing attacks, in which the user fooled into entering password at a fake site.

Passpet [5]improves and combines several previously related techniques password hashing, password strengthening, pet names and UI customization to moderate all the problems just mentioned, helping users to manage website logins more conveniently and more securely. This paper also contributes various ideas in secure interactive design which are separable and that are reapplied in various other contexts which include:(i)Using the user-assigned site labels for the password hashing.(ii)Continuously estimating the malware-attack time when the user enters the new password.(iii)Variable levels of the password strengthening, configured by the user simply by the waiting.(iv)Associating the security tool with the person that differs from a user to user.(v)Customizing the button for activating the security tool in order to prevent spoofing and phishing. After the Passpet[6]Firefox is being installed, the procedure include three steps:

- The user is asked to enter an address[master address] in the form of username@hostname, where hostname identifies a Passpet server.
- A random icon is automatically chosen from the set of animal icons and the random names are given to each animals. The name and icon form Passpet's person for interacting with the user.

The master secret is chosen by the user. A progress bar indicates an estimation of how long it would take for an attacker to guess the secret. The attack time changes when user types the secret and also increases the time when the user waits.

3.CONCLUSION AND FUTURE SCOPE

An authentication protocol against password stealing which make use of cell phones and SMS to prevent password stealing and password reuse attacks. It is assume that each website possesses a unique phone number. It is also assumed that the telecommunication service provider participates in registration and recovery phases. The principle is to eliminate the negative influence of human as much as possible. Through user authentication protocol, user only need to remember a long-term password to protect one's cell phone. Users are free from typing any of their passwords into untrusted computers for login on all websites.

Compared with previous schemes, user authentication protocol against password stealing is the first user authentication protocol which prevent password stealing (i.e., phishing, malware, and key logger) and password reuse attacks at the same time. The reason for it is , user authentication protocol against password stealing adopts one-time password approach to ensure independence between each login. User authentication protocol is fully functional, it consider password recovery and support when users lose their cell phones. They also provide recoverability to our user authentication protocol system with reissued SIM cards and long-term passwords. The performance of login of user authentication protocol is better than graphical password schemes, user authentication protocol against password stealing is acceptable and reliable for its users.

The main advantage of user authentication protocol is it allow users from remember or type any passwords into computers for authentication. Despite of other user authentication, user authentication protocol against password stealing involves a cell phone, which is used to generate one-time passwords and it also include a new communication channel, SMS, which is used to transmit the important authentication messages.

REFERENCE

[1] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A.D. Rubin, "The design and analysis of graphical passwords," in SSYM'99: Proc. 8th Conf. USENIX Securit Symp., Berkeley, CA, 2003

[2] S. Wie Den Beck , J. Waters, J.-C. Birget, A.Brodskiy,and N.Menon"Pass points: Design and longitudinal evaluation of a graphical password system ," Int. J. Human - Computer Studies, vol. 63, no. 1, 2, pp.102–127, 2005.

[3] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient method for Securely managing Passwords,"WWW'05:Proc.14thmWorld Wide Web NewYork, 2005, pp. 471–479, ACM.

[4] A. Perrig and D. Song, "Hash visualization: A new technique to improve real-World security" inProc.Int.WorkshopCryptographic Techniques E- Commerce, Citeseer, 2006, pp 131–138.

[5] K.-P. Yee and K. Sitaker, "Passpet: The most Convenient password management, phishing Protection , " in SOUPS ' 06: Proc. 2nd Symp. Usable Privacy Security, New York, 2006

[6] P.Kasturil.R Kokila-A Novel Security Model For Password Stealing And Password Reuse Attacks,2008,pp.123-132.

AUTHOR PROFILE

Aparna CM is pursuing her B Tech degree in Computer Science and Engineering from MBC College of Engineering and Technology, Peermade, Idukki under Mahatma Gandhi University.

Binisha Mohan is pursuing her B Tech degree in Computer Science and Engineering from MBC College of Engineering and Technology, Peermade, Idukki under Mahatma Gandhi University.

Alpha Vijayan is currently working as an Associate professor in Computer Science and Engineering department in MBC College of Engineering and Technology, Peermade, Idukki under Mahatma Gandhi University. She received ME degree in CSE from Jerusalem College of Engineering under Anna University Chennai.