www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 7 July 2015, Page No. 13574-13577

Efficient Authentication Technique Based On Virtual Password

[1]Sufyan Panginikkadan, [2]Zainul Abid T.P.

[1] M-Tech Student, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
sufyan.kakkad@gmail.com

[2] Assistant Professor, Computer Science and Engineering, MES college of Engineering
Malappuram, Kerala, India
zain.mes6@gmail.com

Abstract: ***The uses of internet in online communication have been increased and the threats against the internet security also increased. Here we discuss how to prevent user's passwords from being stolen by adversaries in online environments. The virtual password mechanism prevents user's passwords from being stolen by adversaries. Here propose a virtual password concept involving a small amount of human computing to secure user's passwords in online environments with the freedom to choose a virtual password scheme ranging from weak security to strong security. However, there is trade-off between simplicity and security conflict with each other and it is difficult to achieve both. Further propose several system recommended functions that provide a security and analyse how the proposed schemes defend against phishing, keylogger, shoulder surfing attacks, and multiple attacks. In user-specified functions, we adopt secret little functions in which security is enhanced by hiding secret functions.***

Keywords: Phishing, Keylogger, Shoulder surfing

1. Introduction

Today The Internet has entered into our daily lives as more and more services have been moved online. Besides reading the news, searching for information, and other risk free activities online, we have also become accustomed to other risk related work, such as paying using credit cards, checking or composing emails, online banking, and so on. While we enjoy its convenience, we are putting ourselves at risk. Most current commercial websites will ask their users to input their user identifications (IDs) and corresponding passwords for authentication. Once a user's ID and the corresponding password are stolen by an adversary, the adversary can do anything with the victim's account, which can lead to a disaster for the victim. As a consequence of increasing concerns over such risks, protecting user's passwords on the web has become increasingly critical.

Many schemes, protocols, and software have been designed to prevent users from some specified attacks. However, to the best of our knowledge, there is not a scheme which can defend against all the attacks listed above at the same time. In this paper, we present a password protection scheme that involves a small amount of human computing in an Internet based environment, which will be resistant to phishing scams, Trojan horses, and shoulder surfing attacks. We propose a virtual password concept involving a small amount of human computing to secure user's passwords in online environments. We propose differentiated security mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security. The trade off is that stronger schemes are more complex. Among the schemes, we have a default method (i.e., traditional password scheme), a system recommended function, a user specified function, a user specified program, and so on. A function/program is used to implement the virtual password concept by trading security for complexity by requiring a small amount of human computing. We further propose several functions to serve as system recommended functions and provide a security analysis. We analyze how the proposed schemes defend against phishing, key logger, shoulder surfing, and multiple attacks. In user specified functions, we adopt secret little functions in which security is enhanced by hiding secret functions or algorithms. To the best of our knowledge, our virtual password mechanism is the first one which is able to defend against all three attacks.
The proposed functions include secret little functions and codebook functions. Our objective is to produce a function achieving both:
1) Ease of computation
2) Security

However, since simplicity and security conflict it is difficult to achieve both. The idea of this paper is to add some complexity, through user computations performed by hand or computation devices, to prevent the three kinds of attacks. There is a trade off how complex the computation by the users can be. One goal is to find an easy to compute but secure scheme for computing. We believe that, for some sensitive accounts such as online bank accounts and online credit card accounts, users are likely to choose additional complexity which requires some degree of human computing in order to make the account more secure.

1.1 Attacking methods

In the Phishing Attack, the aggressor attains the user information, by acting as a responsible person. In the Password Stealing Program Attack, software codes are used to attain the password. The Key Logger Program and Trojan Redirectors are example for password stealing program. In the Key Logger, the software that will be installed on the system

and that software records all the activities done on the key board are recorded. Whenever the user trusts the third party system, that software may be installed on the system. This type of software not displayed on the task manager. From the recorded key, the aggressor gets the password within a short time and less effort. In Shoulder-Surfing Attack, the camera is fixed to monitor all the activities of the user. For this purpose, the hidden cameras are normally used by the aggressor

2. Related works

How to shield users' passwords from being stolen by adversaries is not a new topic, but it is always important because adversaries keep inventing more and more advanced attacks to break the current defense schemes. This results in more research on protecting users from such attacks. In this section, we briefly introduce the previous work on defending against user password-stealing attacks for the three major categories Phishing attacks are relatively new but very effective The author[1] proposed The static password is the most popular authentication method. A password is a secret word or phrase that must be used to gain access to something. That something can either be an application, a network, documents, data or a computer system. Generally, a password should consist of something that is hard to guess, so that it will remain a secret. We call this type of password as "static password" as it does not change and rarely altered. In other word a static method is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource which should be kept secret from those not allowed access. However, with our increasing dependence on the Internet, using static password to gain access to a system is no longer safe. So it's the least secure authentication method. This is because static passwords can be cracked, guessed or stolen. Hackers are getting better each day at cracking sophisticated passwords. Once this happened, they can gain access to your private network and steal your sensitive business information such as your customer database, emails or financial information. The author [2] proposed the secure Authentication in the internet Cafe without Worrying About Keyloggers. The roaming user may use the internet café for browsing. In that system the key logger program may be installed. The author of the system defines the security against key logger program. In this mechanism, the user types a password with an extra character. The software stores all the keys typed on the keyboard .If we type the extra characters then the aggressor got confuses to obtain the password. For example, the user password is trust me, when the user enters it on the untrusted system they type correct password on password field and type random characters on the floor. These random characters and passwords are typed in mixed. The key logger didn't know which characters are typed on the password field and which are all typed on the floor. The result of key- logger is "ftrtewriuksllat34f3plkutm90ehy" for trust me password. The advantage of this system is to secure the password from the Key Logger software. The disadvantage of this system is Shoulder-Surfing Attack is possible. The author [3] proposed graphical user authentication. The graphical password schemes are better than the character passwords. The author of the system [2] explains, this type authentication is complex to hack. It allows Convex Hull Click (CHC) to secure the password. This paper allows a user to select the image from image set. The user may select more number of images that is equal to the number of password characters. The advantage of this system is to protect the password against Shoulder-Surfing Attack. The disadvantage of this system is huge memory is required to store the images and same images are repeated more time. The author [4] proposed the Authentication in social network. Now-a-days the usage of the Online Social Networks (OSN) is increased. In that OSN, the user begin contacts without meet each other. It may cause vulnerability against security. Here the attacking mechanism is known as Impersonation Attack. The aggressor creates an account using another personal details and make communication with each other. In this mechanism, the public key was generated between the two users and it will be exchanged in secure channel (i.e. mobile channel). These public keys are stored on the third-party; whenever the user makes a communication they request a key from the third-party. The advantage of this mechanism is secure in OSN because of third-party authority. The author [5] proposed the One time password for authentication The one time password is valid for one time login and it protect the password against replay attack. The password is based on three approaches that are 1.Time Synchronization 2.Depend on the previous password and 3.Depend on the Challenge. The advantage is, it is a dynamic password and each time new password will be generated. The disadvantage of one time password is time delay and OTP method is difficult to connect via untrusted machine. The Author [6] proposed another secure mechanism is virtual password mechanism. The virtual password is similar to the one time password it was generated by using the secret little function. Differentiated virtual password security mechanism for system registration in which the system allows
users to choose a registration scheme ranging from the simplest one (default) to a relatively complex one, where a registration scheme includes a way to choose a virtual password function. The more complex the registration will be more secure the system and the more user involvement is required. A virtual password is a dynamic password that is generated differently each time from a virtual password scheme and then submitted to the server for 1 authentication. A virtual password scheme P is composed of two parts, a fixed alphanumeric X (i.e., the real password, also called the hidden password) and a function F. Since we call P = (X, F) a virtual password scheme, we call F a virtual password function (VPF). The result (denoted as V) of the VPF is called a virtual password, and F may have some hidden parameters H, which are the secrets between the server and the user.

3. Proposed work

In this chapter an efficient authentication system is introduced which is the modified version of the authentication using virtual password based system. The modification is done in two parts one to add unique security code with mobile application to give more security to the system and other to convert java mobile application to android application. The following section describe the detailed modification steps, the Addition of unique security code and Design phase

3.1 Addition of unique security code

A unique security code can be introduced with mobile application to give more security to the system. In addition to the access code a unique security code is also used for the calculation of the new access code. Only the user can know the unique security code. in the case of online banking environment after the registration of account the user will get the .apk file for download and unique security code. In existing

method only the access code is calculated using secret little function and get the generated code for completing the authentication. In proposed system, access code and unique security code is used with secret little function for calculating the generated code. so the attacker will not get the unique security that only known by the user. so it will give more security to the system.

3.2 Design Phase In Proposed system

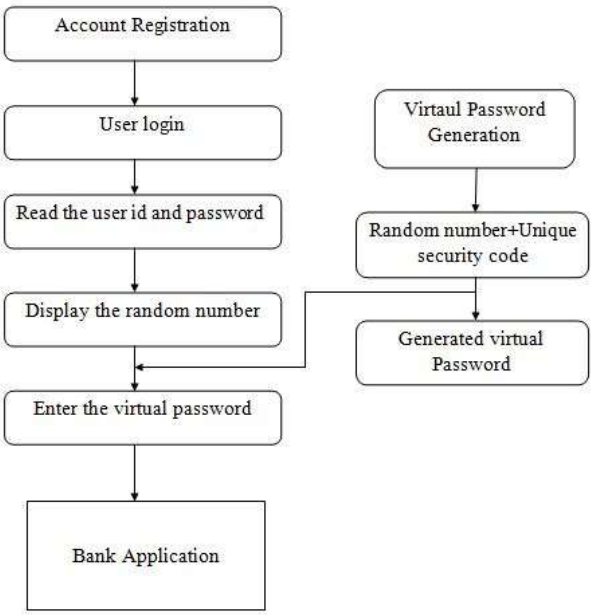

Figure 1: Framework of the proposed system

.

4. Results and Analysis

For the experimental study, here taken around 50 users responses for our system implementation. The user satisfaction for using mobile application in online banking can be modeled as an uncertain object. Implementations were done in Java. From the experimental results it can be seen that, Most of the responders can be use the mobile application for creating virtual password is Very Easy and the security of the virtual password for preventing online attack such as phishing, shoulder surfing, key logger etc. are satisfactory for most of the user. The opinion of the user is addition of unique security code for generating give more security. But the most of the surveyed people showed their need for more secure internet with the cost of spending a little extra time.

Question Analysis	How Comfortable is it to use Mobile application for generating virtual password
Easy to use	68%
Moderate to use	20%
Difficult to use	12%

Question Analysis	Would u like to improve security Little more
More security need	24%
Proposed System is better	52%
Don't care	16%
Yes, But depend on time	8%

Figure 1: Response of users

Figure 1, Represent the users respond for the using comfortability of mobile application for generating virtual password. From the Figure 1, it was found that 68% of the responders can be use the mobile application for creating virtual password is Easy, 20% respondents can use mobile-application for medium level and only 12% responders tell to use the mobile application is difficult and next question analysis it was observed that 24% of responders showed their need for more secure internet, 25% responders tells proposed system gives better security and 16% responders not care about the security and 8% responders need for more secure internet with the cost of spending a little extra time.

5. Conclusion

The virtual password mechanism prevents user's passwords from being stolen by adversaries. Here propose a virtual password concept involving a small amount of human computing to secure user's passwords in on-line environments with the freedom to choose a virtual password scheme ranging from weak security to strong security. However, there is trade-off between simplicity and security conflict with each other and it is difficult to achieve both. Further propose several system recommended functions that provide a security and analyze how the propose schemes defend against phishing , key-logger, shoulder-surfing attacks, and multiple attacks. In user-specified functions, we adopt secret little functions in which security is enhanced by hiding secret functions and it seem to be user-defined functions (secret little functions) are better. In Future we plan study how to improve more security to the system with low computation time.

References

[1] Indu S, Sathya T.N. Saravana Kumar V. "A Stand-Alone AND SMS-Based Approach For Authentication Using Mobile Phones " , Information Communication and Embedded Systems (ICICES).2010

[2] Herley.C, Florencio.D, "How to login from an internet cafe without worrying about keyloggers" in proc. SOUPS, 2006

[3] Widenbeck. SWaters.J, Sobrado.L, Birget.J, "De- sign and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme", Proceeding AVI '06 Proceedings of the working conference on Advanced visual interfaces Pages 177-184 ,2006

[4] X. Zhao,L. Li,G. Xue, "Authenticating strangers in online social networks", Int. J. Security Netw., vol.6,no.4, pp. 237238, 2011

[5] M. Viju Prakash,P. Alwin Infant,S. Jeya Shobana, "Eliminating Vulnerable Attacks Using One-Time Password and PassText", Universal Journal of Computer Science and Engineering Technology , 133-140.2010

[6] Yang Xiao, Chung-Chih Li, Ming Lei, and Susan V. Vrbsky, " Differentiated Virtual Passwords, Secret Little

Functions, and Codebooks for Protecting Users From Password Theft" in *Proc. IEEE ICC*,2014

[7] Ming Lei, Yang Xiao, Susan V. Vrbsky, Chung- Chih Li, and Li Liu " A Virtual Password Scheme to Protect Passwords ", IEEE SYSTEMS JOUR- NAL, VOL.8, NO.2 ,2008

[8] Yang Xiao, Chung-Chih Li, Ming Lei, and Susan V. Vrbsky ," Secret Little Functions, and Code- books for Protecting Users From Password Theft", IEEE SYSTEMS JOURNAL, VOL.8, NO.2.2008