International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 2, No. 2
May 2013

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 2, No. 2, May 2013

Research Paper

DIFFERENTIATED VIRTUAL PASSWORDS FOR PROTECTING USERS FROM PASSWORD THEFT

Kanagaraj S[1], Javith Ibram Sha M[1], Madhan Kumaran D[1] and Rajkumar D[1]

*Corresponding Author: **Madhan Kumaran D,** ✉ madhan.bckin@gmail.com*

People enjoy the convenience of online services, but online environments may bring many dangers. In this paper, we discuss how to prevent users' passwords from being stolen by attackers. We propose a virtual password concept involving a small amount of human computing to secure users' passwords in on-line environments. We adopt user-determined randomized nonstop generation functions to secure users' passwords based on the fact that a server has more information than any attackers does. We analyze how the proposed scheme defends across phishing, key logger, and shoulder-surfing attacks. To the best of our ability, our virtual password mechanism is the first one which is able to defend against all three attacks together. We also implemented the system to do some tests and survey feedback indicates the feasibility of such a system.

Keywords: Differentiated virtual passwords, Key logger, Phishing, Secret little functions, Shoulder-surfing

INTRODUCTION

Today the Internet has entered into our daily lives as more and more services have been moved online. 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 attackers, the attackers can do anything with the victim's account, which can lead to a disaster for the victim.

In this paper, we present a password protection scheme that involves a small amount of human computing in an Internet-based environment or a ATM machine, 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 users' password 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. A function 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

[1] Kumaraguru College of Technology, Coimbatore, India.

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 functions. 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 two other schemes called codebook and reference switching functions. Here the use of these functions are ease of computation and security. The idea of this paper is to add some complexity, through user computations performed by heart/ hand or computation devices, to prevent the three kinds of attacks.

The rest of this paper is organized as follows. Section II, Related works, we describe related work about password protection. Section III, Differentiated Virtual Passwords and Secret Little Functions, we propose the idea of the virtual password, differentiated security mechanisms, and user-specified functions or programs, in which we propose the concept of secret little functions. Section IV, Quantitative Security Analysis, we provide some quantitative analysis. Section V, Implementation and Evaluation, we describe implementation issues of our scheme. Finally, Section VI, we conclude our paper and describe our future work in conclusion.

RELATED WORK

Adversaries keep inventing more advanced attacks to break the defense schemes. This results in more research on protecting users from such attacks. Here we briefly introduce the previous work on defending against user password-stealing attacks for the three major categories. Phishing attacks are new but very effective. There are two types of phishing. First, to prevent phishing e-mails, a statistical machine learning technology is used to filter the likely phishing e-mails; however, such a content filter does not always work correctly. Blacklists of spamming/phishing mail servers are built; however, these servers are not useful when an attacker hijacks a virus-infected PC. Second, to defend against phishing websites, the authors developed some web browser toolbars to inform a user of the reputation and origin of the websites which they are currently visiting. The authors implemented password hashing with a salt as an extension of the web browser, a webproxy , or a stand-alone Java Applet.

Unlike phishing, malicious Trojan horses, such as a key logger, are not attacks, and sophisticated users can avoid them.

Such programs are also easy to develop and there is a great deal of freeware that can be downloaded from the Internet to prevent them. You may be advised to install an antispyware or anti-virus software package on your machine to set up a firewall to block suspicious packages from the outside. Instead of typing your whole password into the login field, the user changes focus outside the login form and types some random characters between any two successive password characters. This trick only makes it slightly more difficult because it is very easy to record all the keys, mouse events, and applications of the focus.

Alphanumeric password systems are easily attacked by shoulder-surfing, in which an adversary can record the user motions by a hidden camera when the user types in the password. The authors adopted a game-like graphical method of authentication to combat

shoulder-surfing; it requires the user to pick out the passwords from hundreds of pictures, and then complete rounds of mouse-clicking in the Convex Hull. The authors proposed a scheme to ask a user to answer multiple questions for each digit. In this way, it is only somewhat resistant to shoulder-surfing because, if an adversary catches all the questions, then they will know what the password is.

DIFFERENTIATED VIRTUAL PASSWORDS AND SECRET LITTLE FUNCTIONS

A. Virtual Password

For authenticating a user, a system needs to verify a user by using the user's password and user ID which the user provides. Both the user's password and ID are fixed. It is reasonable that a password should be constant so that it can be easily remembered. However, the price of being easily remembered is that the password can be stolen by others and then used to access the victim's account.

At the same time, we cannot put password in a randomly variant form because it would be impossible for a user to remember the password. To overcome this, we introduce the new concept of virtual password. 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 authentication. The virtual password scheme contains two parts, a fixed alphanumeric *X* called the hidden password and a function *F*. The server finds it easy to verify the user if *F* is a bijective function. First the server finds the user's record from the database based on the user's ID, then it computes Virtual password and compares it with the one provided by the user. A bijective function makes it easier for the system to use the reverse function to deduce *F*'s virtual password. Therefore, we do not assume that *F* is a bijective function. The user should be free to pick the hidden password. We describe the differentiated security mechanism in the next section to allow the user to choose a Virtual Password Function.

B. Differentiated Security via a VPF

Here we have introduced the concept of the virtual password and next, we detail how to apply it in an Internet-based environment. We propose a differentiated security mechanism for system registration in which the system allows users to choose a registration scheme ranging from the simplest one to a relatively complex one, where a registration scheme includes a way to choose a virtual password function. The system is more secure when the registration is more complex and more user involvement is required.

1. The recommended approach is that after the System receives a registration request it automatically generates a function. The users do not have to provide extra information about the function to the server except for some necessary parameters, called hidden parameters (*H*).
2. The user specified function approach is the one in which users themselves can choose any function they like. However, such freedom is based on the assumption that the user has some basic knowledge about VPFs, which can be introduced by an online introduction.
3. The indirectly-specified approach, instead of letting either the user or the server make the full decision, allows a user to specify the desired security degree. The server will assign a function according to that degree.

4. An extreme scheme is that the user can even provide a program in C or Java instead of a function. It requires a very advanced user.

See to that, except for the default approach, either user computing is involved or a computer which can be programmed to compute the virtual password is needed. Its possible to develop a smart application to make the complex calculation for the user which can be run on the mobile phones like a cellular phone, smart phone, iphone, personal computer, or programmable calculator, to relieve the user from complicated calculations and to overcome any short-term memory problem.

Regardless of the approach chosen, a user's registration in the system is similar that is the user submits a user ID and a fixed password. The one difference from a traditional approach is that in the virtual password scheme, a VPF must be set during the registration phase. The server then delivers this function information to the user via some channels, such as displaying it on the screen or in an e-mail. The user needs to either remember this function together with the password they have chosen or to save them in disks or e-mails. The user-specified password and the system generated function are combined to form a virtual password scheme. A small amount of human-computing is involved in the authentication process. Choose a VPF to make the calculation as simple as possible if the helper-application is not used. Unlike the traditional scheme, users can change the hidden password, the VPF, or both.

C. User-Specified Functions/Programs

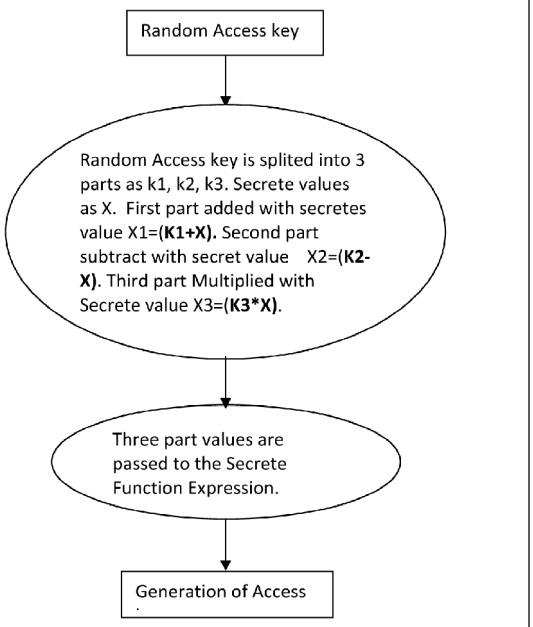
The strongest security approaches let the user define a user-specified function or program. Since the chosen function is only known by the server and the user and the key space of functions are infinite, these approaches are very secure for even simple functions. In many classical ciphers, secret encryption algorithms are common. In modern ciphers, encryption algorithms are open to the public but keys of these algorithms are kept secret. One reason that modern ciphers seldom choose secret encryption algorithms is that secret encryption algorithms prevent communication among parties such as commercial products, networking protocols, and so on.

Therefore, the approach in which only keys are kept as secrets and algorithms are open to the public for implementation is very popular in modern ciphers. The reason for using user-specified VPFs is that secrets are very personal to a particular user and should not be known by others except the server. Therefore, we claim that, for personal communication, such as one between a user and a server, it is acceptable to use secret encryption algorithms. Since even a very simple function will be secure because the attackers do not know what kind of functions the user chose that is functions are kept as secrets. User specified functions can be infinite. The attackers do not know the function forms these simple functions are very secure. Otherwise, it would be easy to attack these functions. These simple and secure functions is termed as secret little functions.

One problem is that extra effort is required in programming the function into the server upon the creation of an account, so human effort that may be needed. The constraint is that secret little functions must use the random number provided by the server; otherwise, it may be subject to Key-logger attacks since the attackers do not need to know the function but can simply input the same capture inputs again to gain access. The users can also define a program to be used.

Figure 1 illustrates the flow chart of user defined program.

Figure 1: Flow Chart of User Defined Program



D. VPF With a Helper-Application

If a helper-application is available, the user needs to type the random salt into the helper-application. Then subsequently, the virtual password is generated by the helper-application. The user then types the generated virtual password in the login screen. By this way, the extra time required is very small and the precision will be 100% correct till the user types the correct random salt displayed on the login screen. This works when the user has a mobile device like cellular phone, PDA, smart phone, iphone. However, such mobile devices are not able themselves to communicate with the server to which the user wants to login. How complex the VPF is, the helper-application can always generate the correct virtual password for the user. This is the most convenient approach for the user. For password changing, the user only needs to get a new helper-application after the password change instead of remembering the changed parts of the virtual password. We need to make sure that the server must make the corresponding changes too.

E. μTESLA Authentication

Here we propose a scheme to guard against phishing attacks by allowing the user to authenticate the server and adopting μTESLA to provide freshness of the server key. The purpose of this scheme is that it can be used for authentication of the server before re-keying of the previous scheme. This μTESLA scheme can be very useful when the web browser or other client side applications, such as the helper-application in our virtual password, can have an authentication function implemented. This scheme can also be used to protect from phishing via e-mails.

μTESLA is an authentication scheme which was originally designed for sensors to authenticate a broadcast message sender in a sensor network based on a public one-way hash function. This μTESLA scheme will work effectively to shield the clients from phishing attacks, and it could be used together with our virtual password scheme to protect the user's password.

QUANTITATIVE SECURITY ANALYSIS

Quantitative analysis is always necessary in security analysis. We express the three common methods of stealing passwords based on the degree of damage they are able to cause. The attacker have different properties that may affect design principles for password protection against them.

1. **Phishing:** This is highly aggressive method, since the adversary can choose fake random numbers to help them figure out the hidden part of the password. The possible key-space dramatically drops after a few successful phishing attacks. Anyway the adversary cannot conduct successful attacks on the same victim too many times because the victim will become suspicious.
2. **Shoulder-surfing:** This attack is less aggressive due to its physical constraints. The adversary may just randomly pick up a victim and obtain some limited data over the victim's shoulder. Even if a camera is well installed at a certain spot, the victims still arrive on a random basis. The adversary has no control over them. But if the virtual password function is not complicated enough, the key-space will significantly drop after a few shoulder-surfing attacks.
3. **Key-logger:** This is the least aggressive attack among the three because the adversary cannot control and observe the random number. It may be safe to assume that the adversary cannot observe the random number provided by the system because the random numbers are shown on the screen and user key/mouse actions usually do not react directly to the numbers. The victim may not be able to know that he/she is under attack that is like a well-hidden Trojan program. Thus, given a sufficiently long period of time, the adversary may collect a certain amount of data for analysis.

Security Analysis for Secret Little Functions

User specified functions can be infinite. Since attackers do not know the function forms these simple functions are very secure. Therefore, secret little functions can easily prevent phishing, shoulder-surfing, key-logger, and even multiple attacks. The secret little function can tolerate an infinite phishing attack. For key-logger/shoulder-suffer the secret little functions can remain secure after the adversary obtains many virtual passwords. We can prove that the proposed scheme can prevent the following attacks.

1. **Phishing:** Since each time, each time the user inputs a virtual password, the phishing attacker could get the virtual password, but cannot obtain the real password. The virtual password is different each time.
2. **Shoulder-surfing:** Since each time, each time the user inputs a virtual password, the shoulder-surfing attacker could get the virtual password, but cannot obtain the real password. The virtual password is different each time.
3. **Key-logger:** Since each time, each time the user inputs a virtual password, the Key-logger attacker could get the virtual password, but cannot obtain the real password. The virtual password is different each time.
4. **Replay Attack:** The virtual password does not suffer the replay attack since each time, the server generated a different random number.

IMPLEMENTATION AND EVALUATION

We implement secret little functions and demonstrate that they defeat phishing, key-logger, and shoulder-surfing attacks in a PC machine. Even though such a calculation is complicated for some people, our helper-applications help to relieve the users of this required human computing. A user response test in the next is to

test the user's feeling on the time spent to calculate the virtual password. Our password scheme is dynamic and requires a user to make some computations. It was found that most of the users could complete the single digit calculation easily without help from the calculator. The need for more secure internet is delivered with the cost of spending a little extra time.

CONCLUSION

We discussed the challenges of protecting users' passwords on the internet and presented some related work in this field. We discussed how to prevent users' passwords from being stolen by adversaries. We proposed a virtual password concept involving a small amount of human computing to secure users' passwords in online environments. We proposed differentiated security mechanisms in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security.

However, since simplicity and security conflict with each other, it is difficult to achieve both. We further proposed several functions serving as system recommended functions and provided a security analysis. We analyzed how the proposed schemes defend against phishing, key-logger, shoulder-surfing attacks, and multiple attacks. In user-specified functions, we adopted secret little functions in which security is enhanced by hiding secret functions/algorithms. In conclusion, user-defined functions (secret little functions) are better., In the future, we plan to study how to design smarter functions to alleviate the computation-burden of the user. We would also like to develop some small applications with built in virtual passwords, which will be able to run at a customer's wireless device, such as a cellular phone or a PDA. With such an application, the user only needs to input the system random digits which the system provides and then the virtual password is automatically calculated for the user.

REFERENCES

1. Anna Lysyanskaya, Roberto Tamassia and Nikos Triandopoulos (2007), "Multicast Authentication in Fully Adversarial Networks".
2. Anti-Phishing working Group [online] available at http://www.antiphishing.org
3. Boneh D and Frankiln M (2003), "Identity-Based Encryption from Weil Paring".
4. Cheng N, Govindan K and Mohapatra P (2011), "Rendezvous Based Trust Propagation to Enhance Distributed Network Security ," *Int J. Security Netw* ,Vol. 6, Nos. 2-3, pp.101-111.
5. Choi T and Acharya H B (2010)," Is that you? Authentication in a Network without Identities," *Int J .Security Netw ,*Vol. 6, No. 4, pp. 181-190.
6. Christophe Tarta andHuaxiong Wang (2009), "Efficient Multi Stream Autencation for the Fully Adversarial Network Model".
7. Du W, Deng J, Han Y, Chen S and Varshney P (2004), "A Key Management Scheme for Wireless Sensore Networks Using Deployment Knowledge", in INFOCOM.
8. E Jung .Passwordmaker[online]. Available: http://passwordmaker.mozdev.org.
9. Herzberg and Gbara A (2004), "Trustbar Protecting Web Users from Spoofing and Phishing Attacks".
10. Jiang Y, Lin C, Shi M, and Shen M (2006), "A Self Encryption Authentication Protocol for

Teleconference Services", *Int J. Security Netw.*, Vol 1, Nos. 3-4, pp. 198-205.

11. laur S and Pasinin S (2006)," User-Aided Data Authentication ," *Int J. Security Netw*., Vol. 4, Nos. 1-2, pp. 69-86.
12. Lei M, Xaio Y, Vrbsky S V and Li C C (2008), "Virutal Password Using Random Linear Function for On-line Service," December.
13. Ming Lei, Yang Xiao, Susan V.Vrbsky, Chung-Chih Li and Li Liu (2008), " A Virtual Password Scheme to Protect Password".
14. One-Time Password [online] Available: http://en.wikipedia.org/wiki/One=time_password
15. Pradip D E, Sajalk.Das and Govindan K (2009), "Epidemic Models, Algorithms and Protocols in Wireless Sensor and Ad-hoc Network".
16. Richard M, Guo Ming Lei and Xaio Y (2007), Stranger Danger and the Online Social Network.
17. Roth V, Richter K and Freidinger R (2004), " A PIN –Entry Method Resilient Against Shoulder –Surfing", in Proc .11th ACM Conf .Comput .Communu .Security, pp. 236-245.
18. Sharma M J and Leung V C M (2011), "Improved IP Multimedia Subsystems Authentication Mechanism for 3G-ALAN Networks".
19. XinxinZhao, Lingjun Li and GuoliangXue (2010) , "Authenticating Stranger in Fast Mixing Online Social Network".
20. Y.Xaio C-C, Li M Li and Vrbsky S V (2008), "Secret Little Functions and Codebook for Protecting Users from Password Theft," in Proc.IEEEICC, May, pp. 1525-1529.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com