A SURVEY ON SECURE VIRTUAL PASSWORD AND PHISHING ATTACK

Ms. Himadri Tank[1], Mr. Vinay Harsora[2]

[1]M. Tech (CE), Second Year, RK University, Gujrat, India,
[2]Asst.Prof. RK University, Gujrat, India

Abstract: Nowadays, Most Commercial website offers on line services like net banking, on line payment, online shopping for people convenience. Online services require user ID and password for authentication. The peoples use mostly easy to remember password and these passwords are easily stolen by different attackers. There is a need to provide strong password scheme for password, but strong password are hard to remember. To conquer this problem virtual password scheme was introduced. This paper includes a detailed survey on different secure virtual password scheme, phishing attack concept and some techniques to defend against phishing attack through different virtual password scheme.

Index Term: Virtual Password, Secret little function, Phishing attack

I. INTRODUCTION

With the use of online transaction like online payment with credit cards, email conversation, net banking may invite some harmful task. Such online transactions require user identification and subsequent password. Generally, password schemes do not use random number because it is difficult to remember. Transport Layer Security and Secure Sockets Layer are basically cryptographic protocols designed to provide communication security over the internet [1], but it is based on plain text password and user ID. Again these authentication is easily stolen by some attacks including phishing, malicious Trojan horses, shoulder- surfing [13], malware (record the keystrokes) based attacks [15].

A one-time password avoids fixed password scheme since it generates a password which is valid for only one transaction [17]. A one-time password which is valid for only one transaction (OTP) provides security against replay attack because it is not fixed password. A time-synchronization method of OTP method requires the token and the computer system. Both are used to generate numeric version of current time which is then run it through algebraic process, but using OTP it is difficult for user with un-trusted machine [18].

Predefined encryption algorithm are based on conventional cipher and in modern ciphers keys are kept to secret. However, these authentication processes are at a standstill susceptible to known attacks like phishing attack, password stealing Trojan programs and shoulder surfing, key loggers, mobile malware attack.

Another online transaction on the internet referred as online banking is an electronic

banking system allows user to access easily to their banking activities such as retrieving an account, history record of online transaction. To access online banking facility users have to register with their websites and need to set up password for user authentication. So, here user must keep their password as secret as being stolen by any adversary.

How to crack user password in online environment is not a new thing, but it has become an interesting research area. There are no of attacks like phishing attack which is continual threat, an example of phishing of cooperative commerce techniques used to mislead users, to crack the current web security technologies [3]. A famous method of thieving people password and personal information by capturing users shoulders using hidden camera [16]. A software application, Trojan Redirector [10] was designed to redirect end-users network traffic to a location to where it was not intended. This includes crime ware that changes hosts and other DNS specific information, crime ware browser-mobile objects that may install a network level driver or to redirect users to fraudulent locations [8].

Commercial websites require user ID for registering and password for user authentication. A system verifies a user using the user's unique ID and hidden password which is provided by the user. In this scheme user's ID and password are static, easily remembered, can be stolen by others and then used to crack the user's account. Furthermore, static password cannot take random number since it is difficult to remember. There is a need to change or add some complexity in static password system. There is no of applications to create strong dynamic password generator, virtual password generator, but all are based on conventional encryption algorithm.

A. Virtual Password Scheme:

To deal with above mentioned challenges, by [5] virtual password scheme can be used. A virtual password concept is based on arbitrary string, generated differently each time and further returned to the server for authentication.

A virtual password P is composed of two parts, a fixed alphanumeric X containing hidden parameters given by the user and a function F from S to S, where the S is the letter space which can be used for passwords. So, virtual password P is defined as (X,B) where hidden parameters X=x1,x2,x3,x4….xn ,xi£Z ,Z will be the all password characters and B (F,R) where R=r1,r2,r3,r4….rn. Some human computing is needed to generate virtual password based on after user registration system will pop up function that could use random salt and hidden parameters. In addition to this scheme, a secure method has been proposed with differentiated virtual password scheme [12] including secret security level from lower to higher provide by secret little functions with system recommended function, user specified approach and indirect approach.

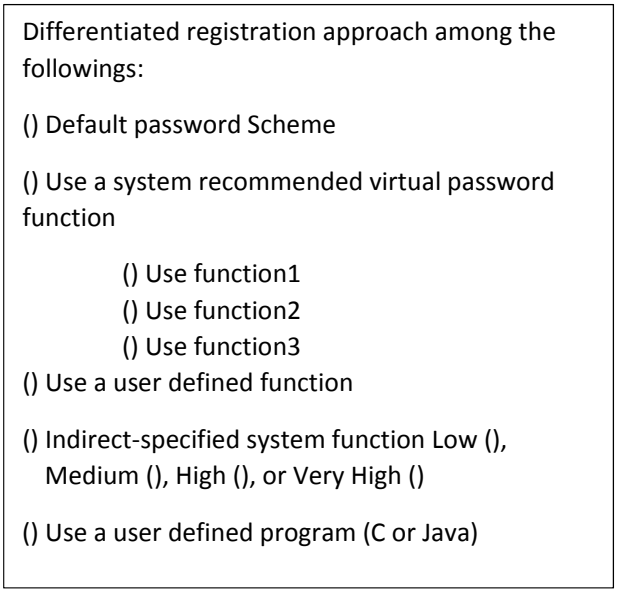

Fig 1. Differentiated Virtual Password Scheme Registration

Above figure shows a differentiated 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. For user authentication server needs to verify the user if F is a bijective functions. If F is not a bijective function, than the server has to find the user's record from the database on the user's ID, then it computes virtual password and compares it with the one provided by the user.

B. Phishing Attack:

Phishing is a frequent threat that keeps growing to this day. Phishing is the way of acquiring vulnerable information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication and Email spoofing and instant messages are web application in which phishing are typical carried out [3].

Various types of phishing attacks have now been identified like deceptive phishing, Malware – based phishing, Key loggers and Screen loggers, Session Hijacking. With phishing user cannot identify whether the website is fake or real.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password credit card, social security or bank account numbers. The website, however is bogus and set up only to steal the information which user enters on the page [21].

II. LITERATURE REVIEW

A lots of techniques have been discovered and defined to defend against phishing attack. The following section gives a brief review of various technique for the same and virtual password scheme.

Through phishing email users are directed to visit a bogus website where they are asked to update sensitive information such as a password, credit card or bank account numbers. Spam Assassin [9] is a computer program released under the Apache License 2.0 used for e-mail spam filtering based on content-matching rules, in which the program can be integrated with the mail server to automatically filter all for a site. It can also be run individual users on their own mailbox and integrates with several programs. These servers are not useful when an attacker hijacks virus-infected PC.

To deal with junk email M. Shahami [14] automated construction of filters to eliminate unwanted mail form the user mail stream using Bayesian classifier, a Bayesian network applied to classification task. They included approximately 20 non-phrasal, domain specific features into their junk e-mail filter.

An application, APS RBL is a real-time black hole list [21] with the use of DNS list to identify hosts which have been coupled with the sending of spam mail. Companies and ISPs can acquire from which IP addresses to obstruct traffic. Unwanted emails can be prevented using multiple black hole services. However blacklists of spamming/phishing mail servers are not useful when an attacker hijacks a PC and specified system require regular administrator.

By [6], a flexible sender validation small fry is a validation practice for sending some kind of fake email address. This system uses unneeded copies of IP data to permit both efficient use by very high-volume mail servers and simple implementation on low to moderate volume mail servers.

A re-encryption scheme [2] that recognize a stronger notion of security and proxy encryption as a method of adding access control to a secure file system.

Trust Bar [11] is a secure user interface add-on to browsers. It identifies the site and the certificate authority. To prevent unwanted pages Trust Bar displays highly visible warning. For defending against phishing websites, they developed some web browser toolbars to inform

a user of the reputation and origin of the websites which they are currently visiting. Phishing filters and toolbars are designed to protect the web surfer from collectively engineered phishing scams which try to trick the intended victim into visiting a fraudulent website disguised to look like a valid e-Commerce or banking site.

The Net craft Anti-phishing [20] toolbar is a community-based reporting indicative which gives higher weight to report from expert or highly trusted users. This helps ensure rapid discovery and prevention of newly discovered phishing sites while lowering the potential for false positives.

In [4] a browser extension, password hashing technique that transparently produces a different password for each site, improving web password security and defending against password phishing and other attacks, the authors implemented password hashing. It is an extension of the web browser, a web proxy, or a stand-alone Java Applet.

Diffie-Hellman protocol [7] which is also known as exponential key exchange is one kind of digital encryption for establishing a shared secret over an unsecured communication channel and first published by Whitfield Diffie and martin Hellman in 1976.

One time password [17] is valid for one time login and it protects the password against replay attack. One password is based on approaches like time synchronization and depend on the challenge. The advantage is, it is a dynamic password [18].

In [5] a new way of protecting users from adversary, a virtual password scheme was introduced. This scheme include small amount of human computing for security purpose and can be used for authentication. They have adopted user determine randomized linear generation function. The user hidden parameters and system generated function are collectively formed into virtual password.

Defend against Phishing Attack using virtual password:

The virtual password scheme to protect user from password theft with randomized linear function for phisher where c, a, x1, x2, are unknown. They only know k1, k2, k3….. kn, y1, y2…yn. And this scheme can remove the possibility of multiple attack.

Among differentiated virtual password scheme [12] authors also purposed two other schemes codebook and reference switching. These schemes can defend phishing attack by secret little function. Since each time the system read only virtual password, the phishing attacker could get virtual password but it could not get hidden parameters.

III.CONCLUSION

The survey of this paper makes knowledge about the most aggressive password stealing attack and protection method available for the online network communication. The protection of the password is a critical thing in online system. Using different schemes for virtual password mechanism for online transactions people can prevent their password being stolen. In future we try to implement new mechanism from this survey that makes help to provide security against phishing attack.

IV. REFERENCE

[1] Allen, Dierks and C. " The TLS Protocol Version 1.0 ." *IETF RFC 2246* (Jan.1999).

[2]Ateniese, K. Fu, M. Green, and S. Hohenberger. "Improved proxy re-encryption schemes with applications to secure distributed storage, ." *Proc. 12th Annu. Netw. Distributed Syst. Security Symp.* (2005).

[3]Available http://en.wikiPedia.org/wiki/Phishing

[4] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell. "“Stronger password authentication using browser extensions,” ." *Proc. 14th USENIX Security Symp.* (n.d.).

[5] Chung- Chih Li, Ming Lei, and Susan V. Vrbsky. "Virtual Password Scheme to Protect Passwords Communications ." *ICC '08. IEEE International Conference* (May 2008).

[6] Damiani, S. D. C. di Vimercati, S. Paraboschi, P. Samarati, A. Tironi, and L. Zaniboni. "Spam attacks: P2P to the rescue." *Proc. 13th Int. World Wide Web Conf pp. 358359.* (2004).

[7] Diffie, W. and Hellman. ""New directions in cryptography"." *IEEE Transactions on Information Theory 22 (6): 644–654. doi:10.1109/TIT.1976.1055638.* (1976).

[8] "Government Minister avoids the train over visual data security fears"." (January 2013.).

[9] mason. "filtering with spamAssian." *Hetnet* (2002).

[10] C.Herlley and D. Florencio,"How to log in from internet café without worring about key loggers" in proc SOUPS, 2006

[11] Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler. "SPINS: Security protocols for sensor networks,." *Wirel. Netw. vol. 8, no. 5, pp. 521534* (2002).

[12] Yang Xiao, Senior Member, IEEE, Chung-Chih Li, Ming Lei, and Susan V. Vrbsky. "Differentiated Virtual Passwords, Secret Little Functions, and Codebooks for Protecting Users From Password Theft ." *IEEE SYSTEMS JOURNAL, VOL. 8, NO. 2* (JUNE 2014).

[13] "A PIN-entry method resilient against shoulder-sur_ng, ." *Proc. 11th ACM Conf. Comput. Commun. Security* (2004).

[14]Sahami, S. Dumais, D. Heckerman, and E. Horvitz,. " A Bayesian approach to flter junk e-mail learning for text categorization ." *Proc. Workshop* (May 1998.).

[15] Shimna M. S., Sangeeta P S. "Dynamic password schemes for protecting users from password theft ." *international journal of innovative technology and exploring engineering* (june 2013).

[16] "shoulder-surfing." *Proc. 11th ACM Conf. Comput. Commun. Security,pp. 236245. 22* (2004).

[17] Sivalingam, Lee and K. M. " An e_cient one-time password authentication scheme using a smart card, ." *J. Security Netw., vol. 4, no. 3, pp. 145152* (2009.).

[18] "An efficient one-time password authentication scheme using a smart card, Int. ." *J. Security Netw., vol. 4, no. 3, pp. 145152* (2009).

[19] Whateley, A. Meyer and B. "SpamBayes: Eective open-source, Bayesian based, e-mail classication system ." *Proc. CEAS* (2004).

[20] Antiphishing working group http://antiphishing.org