DESIGNING AND IMPLEMENTING VIRTUAL PASSWORD TO PROTECT USERS FROM THEFT OF PASSWORD

S. R. SRIRAM, D. SAVEETHA

SRM UNIVERSITY, Kattankulathur, Chennai, TN, India

Abstract— In present days, people are using the online environment to make their work easier. But, this online environment has more risks and security flaws that affect users and retrieve all confidential information about them, and try to attack. So to avoid it, we have planned to implement and develop applications in such a way that they provide secure transactions and protect from adversaries and hackers. To the best of our knowledge, this mechanism is the first one that can defend against most of the vulnerable attacks such as Phishing, Key-Logger and Shoulder Surfing. We have also adopted a scheme μTESLA authentication for re-keying and defending against phishing. This mechanism helps the people and it reduces the time and enhances security in online environment and ATM services.

Keyword—Mobile/ Helper Application, Virtual Password, Secret Little Function (User Specified Function), μTESLA authentication, Phishing, Key- Logger, Shoulder Surfing.

I. INTRODUCTION

Internet has become a part of everyone's life, people could do work efficiently and easily. One of the major processes that people enjoy using internet is online environment, where people enjoy the convenience of online services they are provided, but at the same time they are not aware of the adversaries and hackers, who steal the personal and confidential information of individuals and make them as beneficiaries. So in an online environment, there is a lack of security which leads to many problems.

Even though more security measures are improved in online environment, still hackers find a path to enter to one's personal data and make them vulnerable to attack. Some of the common attacks are phishing, key-logger, shoulder surfing are not having proper security measures to prevent them from users. Till today we are being attacked and suffering from all the above three social engineering attacks. To overcome it, we use virtual password mechanism to defend against them.

In this paper, our virtual password scheme is the first to protect and defend against all the major attacks over the internet, thereby enhancing security level of user. **The main objective of our project is to produce an ease of computation and security to passwords and all confidential data in online environment that should not get hacked**. So our ultimate goal is to design a zero-knowledge interactive providing protocol.

The rest of the paper is organized as follows. We describe about the scope of password protection in section II. In section III, related work for protecting the user's password is done. Then comes to section IV, discussion about mobile/helper application, virtual password, μTESLA authentication and user defined function. In section V, we provide some quantitative analysis and in section VI implementation and section VII, covers conclusion and future enhancement.

II. SCOPE

A small application is developed as a helping application for the users with built in process for calculating virtual password, which will be run at customer's wireless devices such as mobile phones, PDAs, etc.,. With the help of that application, user needs to input the random digits that are generated by the system and this application will calculate a virtual password automatically to the user.

This process is more secure for the people in an online environment, since the virtual passwords are not visible to any of the adversaries/ hackers and thus provides security to users, where the idea of our virtual password is similar to OTP, but their approaches are different. One- time password use dynamic password, and so prevents relay attacks. In OTP, communication is established between the server and a physical device, but in proposed user defined function approach, the functions are built between server and user. OTP assumes that the physical device is secure and not compromised, but whereas secret little functions method does not need such an assumption. So our method is used easily and safely.

Some of our major scopes for developing this project using virtual password mechanism are as follows: i) reduce the burden of the user and provide them a secure environment: ii) protect from all social engineering attacks, especially from phishing, key-logger and shoulder surfing: iii) no hacker can detect user password since it is a dynamic virtual password; iv) most of the people need secure internet with less time and cost.

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

III. RELATED WORK

In this project, an application is developed for all the end users to protect their password and to give them a secure channel in an online environment. Previously, they followed a traditional challenge- response protocol; where the user sends his/her identity to the server, and it generate and returns a random number as a key and as a challenge and user responses as f(r, h (p)). Where f () - function, h () - hash function, p- password; which is not safe, it takes long time to compute and needs human calculation and can be hacked easily.

Whereas, here it includes secret little functions and μTESLA authentication. Some complexities are added in such a way that they protect and prevent all three attacks. During this process, if the user access online in public environment he/she can calculate the virtual password from the random number generator that are generated by the server to the user, so they are not exposed to key-logger and shoulder surfing.

In [1] concept of system and usability were proposed, where user can quickly adapt the system. Virtual password concept is proposed where the server and user share a virtual password which was composed of two parts; 1) a fixed secret password and 2) for each login section server will generate a random based which user enter a virtual password to clear the authentication process. Author considered secret key is fixed part and in [2] author propose that an attacker can recover an equivalent password with only two (or a few more) observed login session.

A virtual password demo is developed [4] where, when the password form appears to user and they move across the squares to generate a random sequenced alphabet and here letters get changed once user click a letter. It is impossible to steal passwords b key logging, shoulder surfing but attacked by phishing and their technique is very complex and so user's find difficult to use it. In [5] an online virtual keyboard is developed, where it is designed to protect password from malicious spyware and Trojan programs. In [6] author proposed a technique by limiting the number of times for login session to prevent replay attack, spoofing attack, dictionary attack.

Generally phishing and key-logger are not attacks, users can easily avoid them. Basically, there are more freeware's hat can be downloaded from the internet to prevent them. Essential things like installing an anti-virus software, setup firewall blocks to avoid suspicious intruders from the outside environment can be done. Avoid responding to unnecessary adversaries i.e., the blogging's that pop out during any online process that we undergo. We may even have a very strong password with all special characters, alphabets and numbers but then they are attacked by shoulder surfing and key-logger. Also more complex the password, the user has to remember them which are difficult.

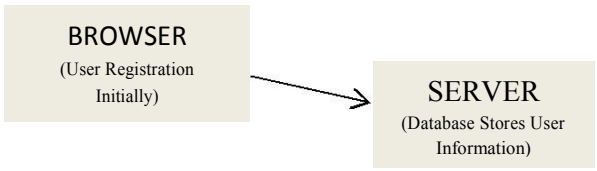

Fig 1. Initial process between user and server

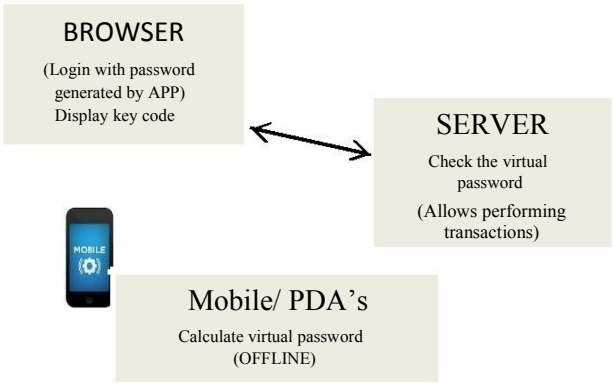

Fig 2. Key code is calculated and a virtual password generates

In our virtual password mechanism, fig 2 every online user will get the dynamic virtual password from a mobile/ helper application, which acts as a calculator but with secret little functions. Firstly, during the online transaction process, for new users they have to make registration with all their essential details and it has to be verified by server and a confirmation mail will be sent to user. Then the user has to complete the process by verifying the mail link.

Then, after the registration process, it will ask regarding the type of operating system the user mobile works with. From fig 1, after that it will be asking the user to download and install an application that the server generates, so called the helper application. The user then downloads and installs it to their PDAs/ mobile phones.

Then, during login process, the user will be asked to type their default username and password they created initially during registration process. If the username and password matches, a random key will be sent by the server to the access page that is visible to the user. Now, the user has to open the helper/ mobile application that they have already installed and enter the key code and then click on calculate. As per the user's expression, calculation will be done and viewed in the access code text field. In the application module, the application will be built with different expression calculation for different users. All the users application are not unique, they varies.

Now the application will calculate a virtual password and the user has to just enter the password to access the page and click OK. The server calculates the password and verifies with that of the password user calculated and entered. If the password is correct, then the user can perform all their online services, transactions safely. If the

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

user doesn't have the corresponding application, they are not able to perform the online services. User can also use Emulator in their computer and run the application in the absence of the hand device.

The virtual password mechanism includes, a virtual password concept where no more human computing is necessary to secure user password in an online environment. They are mainly used with a tradeoff between security and complexity. Several functions serving as systems recommended functions provide a security analysis. We analyzed how the virtual password mechanism defend against phishing, key-logger, shoulder surfing and multiple attacks. In the user-specified functions, we adopted secret little functions, in which security is enhanced by hiding the secret functions/ algorithm. So, user-defined functions (secret little functions) are better. μTESLA authentication is used for re-keying and defending against phishing. Since, for a server it is easy to verify the user's password and authenticate the transaction.

IV. MOBILE/ HELPER APPLICATION, VIRTUAL PASSWORD, USER-DEFINED FUNCTION, μTESLA AUTHENTICATION.

A. Virtual password generator using mobile/ helper application

The application is available for the user, where the user needs to type the random key code generated during the process of performing online transactions in their application that was downloaded during the initial registration process in online environment and press the calculate button and that generates a dynamic virtual password for the user. Usually, this works when the user has a mobile device such as mobile phones, PDAs, however such mobile devices are not able to communicate with server to which the user wants to login. No matter how complex the virtual password function is, the application can always calculate and generate the correct dynamic virtual password for the user. This is a sophisticated one, and it is also the most convenient approach for the user.

We need to enter the generated virtual password in the online access page where the virtual password encoded is verified by the database server and if it matches we can perform online transactions safely. Then whole process that takes place inside the application is not transparent to the user and hacker, so it is more secure.

B. Virtual password

A virtual password is a password which cannot be applied directly but instead generates a dynamic password which is submitted to the server for authentication. For a virtual password, human computing is involved or a handhold device is essential to compute the dynamic password. We could develop a smart application to make the complex calculation for the user, which can run at the mobile device, such as a cellular phone, PDA, personal computer, or programmable calculator, to relieve the user from the complicated calculations and to overcome from providing a very strenuous password which makes problem for user to remember. If such a helper-application is involved, we should make sure that the helper-application is unique to each user account and only work for the corresponding user account. For a server it is always easy to verify the user and also compare the virtual password with the one user provides, so virtual password is the best mechanism to provide security to the user.

C. User defined function

A secret little function or user defined function are those where, even a simple function will be more secure because, hackers do not know what kind of functions the developer choose i.e. functions are kept as secret instead of keys and resulting function space is infinite. User specified functions can be infinite. Since attackers do not know the function forms and so secure. Otherwise, it would be easy to attack these functions; we call these simple and secure functions as secret little functions.

Usually, these secret little functions and algorithms are more secure than encryption technique. In encryption, data are kept confidential, but hackers can easily predict and find by using either brute force attack or by dictionary attack. But secret little functions are kept secret and confidential by the server and is not revealed, even the user/ admin are not aware of what functions are used inside the application for calculation. For every user the application function differs so, it is very difficult for hackers and more secure to users. In this process, the communication takes place between user and server, where no other interactions takes place. Generally it is very harder for a hacker/ attacker to compromise the server and reveal the information.

D. μTESLA authentication

μTESLA authentication is used for re-keying and defending against phishing attack, so we propose a scheme to guard against phishing attacks by allowing the user to authenticate the server and adopting μTESLA to provide freshness for the server key and so the same key will not be generated. This scheme can be very useful for the user, who uses browsers at internet cafe or outside systems. They can also prevent phishing attacks that take place via emails. They will work efficiently to shield the clients/ users from phishing attacks and it could be used together with our virtual passwords scheme to protect the users password.

V. QUANTITATIVE SECURITY ANALYSIS

A quantitative security analysis is generally for providing a list about the process to defend all three major kinds of attacks. All the attacks are more vulnerable and harmful to users, and these attacks are increasing in their number yearly and not minimized. Let us discuss about each attack in brief as follows.

1) *Phishing.* Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

in an electronic communication. It is a simple concept where hackers attempt to trick the victims for disclosing their personal details, bank account details.

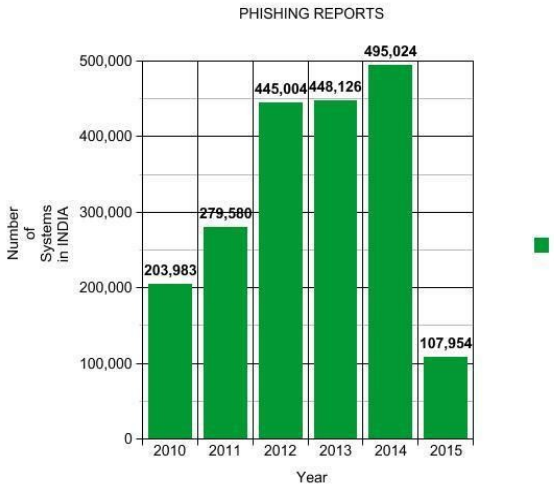

Table 1. Phishing Reports till Feb 2015

By which hacker attack, gather information and get access to user's sensitive data, financial data and bank accounts. Still phishing attack has not come to an end and many systems are getting affected daily, table 1, indicates till today many users are being attacked by this attack as per the source from internet. So our primary idea of this project is to get rid from phishing attack.

2) Key-Logger. Key logging is an action that records keys that are pressed by the users in keyboard to retrieve their password for attacker benefits. This attack usually takes place where user access internet in public/ browsing centers and they are not visible to users. Avoiding this type of attack is not so simple, because the helping software is available in the online market, and they are in the form of software and hardware. So, by using our virtual password mechanism we can prevent from this attack, since the password typed over is a random password calculated by a helper application.

3) Shoulder Surfing. Shoulder surfing is just a technique that is usually followed to know others confidential data like password, PIN, address, contact umber by just looking over someone's shoulder. This attack is done by people and also by adversaries who are in the online services. They monitor user's actions and try to collect information. This attack is impossible to avoid but can be prevented by our technique, since the value is generated by a helper application and it is a dynamic virtual password, so for next time it can't be used.

4) Encryption. Encryption technique is a basic process which encrypts the actual text and is not visible. This technique is used in our project as an additional security, where user enters their username and password initially for authentication/ identification. This username and password is encrypted and sent to server so hacker finds arduous to retrieve username and password.

VI. IMPLEMENTATION AND EVALUATION

We have implemented the secret little functions and demonstrated that this mechanism defends against phishing, key-logger, and shoulder surfing attacks. Here the user just simply types the virtual password that is calculated and generated by the helper application which was developed previously for every user at the initial stage of user registration, so it makes the work of the user more simpler and easier, at the same time enhances security level. Most of the people show their need for more secure internet with less cost.

We implemented this project as the process, where initially for a new user, a registration process is required. Then the access page redirects to next page where it asks about operating system user mobile functions, and the server will ask to download and install that application that server provides. Afterwards a mail will be sent by server to user for confirmation with default password, if needed user can change their password. After all the confirmation process is over, now the user login with their password and username which is encrypted and sent to server for verification, if it matched webpage redirects to next access page for the second step verification where a key code is displayed and a password is asked to enter for confirmation. Now the user has to open the mobile application (which they previously downloaded during registration) and enter the key code and click on calculate. The helper application will calculate and generate a dynamic virtual password, and this password has to be entered in access page by user and then proceed. This virtual password is sent to server and server verifies and allows user to perform transaction.

This helper application runs in offline mode, and this application will not reveal the calculation mechanisms that are used inside to calculate the dynamic virtual password. If user forgot/ delete this application, they can retrieve a new helper application by providing some security steps that are questioned by the server to acquire it. So this technique is more secure and prevents from all social engineering attacks.

VII. CONCLUSION AND FUTURE ENHANCEMENT

We discussed about security measures that lacks in online services, so we proposed a mechanism and developed the application with secret algorithms that prevents users passwords from theft by hackers/ adversaries. We also adopted certain authentication techniques, encryption techniques and provided a security measure for users. This technique defends against phishing, key-logger and shoulder surfing that are some of the major attacks which have to be prevented from hackers. We insist users not to provide/ share any personal details to untrusted advertisements, promoting mails, etc., unless user thinks they are trusted.

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

In future, we plan to demonstrate the process of developing a helper application developing machine or a device for each user, at every time when new user creates a new account. Instead, an auto generator of helper application have to be developed where, it will develop and provide different helper application with various secret little calculation/ functions to the user and sends the data regarding user and the type of helper application to server or a separate device with a link to servers. So this makes work easier, efficient and more secure.

REFERENCES

[1] "Virtual password using random linear functions for Online services, ATM machines, and Pervasive computing", M. Lei, Y. Xiao, S. V. Vrbsky, Communication, pp. 4367- 4375, 2008

[2] "Breaking randomized linear generation functions based virtual password system", Shujun Li, IEEE International Conference on Communications (ICC), 2010

[3] "Review of Password protecting mechanism", Ms. K. Banu priya and Dr. P. Venkateswari, Int. Journal of advanced research in computer engineering & technology (IJARCET) Vol 2, Issue 2, Feb 2013

[4] "Virtual password", D. Rijmenants- planet source code, http://www.planet-source-code.com/vb/scripts/ShowCode.asp?txtCodeId=56714&lngWId=1

[5] "Online virtual keyboard: secure passwords from keyloggers", Dheeraj Bansal- shoutmealoud, http://www.shoutmeloud.com/online-virtual-keyboard-secure-passwords-from-keyloggers.html

[6] "A secure one-time password authentication scheme using smart cards without imiting login times", S. Lee and K. M. Sivalingam, International Journal on Security Networks, 2009

[7] "Dynamic password schemes for protecting users from password theft for E- banking", Shimna M S, Sangeetha P S, Int J. innovative technology and exploring engineering (IJITEE), Issn 2278-3075, Vol 3, Issue 1, June 2013

AUTHORS

S. R. SRIRAM received the B. Tech degree in Information Technology from Anna University, Chennai, India.

Pursuing M.Tech in Information Security and Cyber Forensics at SRM University, Kattankulathur, Chennai, Tamil Nadu, India.
E-mail: sriramsr2506@gmail.com

SAVEETHA D working as an Assistant Professor (O.G) department of Information Technology at SRM University, Kattankulathur, Chennai, Tamil Nadu, India.

ISSN: 2278 – 1323 **All Rights Reserved © 2015 IJARCET**