International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 5, Issue 1 (Jan-Feb 2017), PP.43-46

THREE-FACTOR AUTHENTICATION FOR PREVENTING PHISHING ATTACKS IN BANKING

[1]MOHAMMED MUDASSIR VARDA
Student,SITE School, VIT University
[2]UMA MAGESWARI
Student, GTEC, Anna University
[3]ANUSHA GIRI
Senior Sofrware Developer,FireStream WorldWide Inc., Chennai, INDIA
[4]SANGEETHA PRIYA
Chennai, Accenture
[1] mudassirsmk27@icloud.com

***Abstract* - Today, everything has been digitized and Banking is one of the sectors which faces online threats and Phishing is one of the threat. Phishing is an online uniqueness fraud, which intends to seize classified data mainly alias name, keys and online trading aspects from its sufferers. Primarily, an intruder cheats people to disclose sensible data by emailing a fraudulent broadcast to huge number of customers. Therefore, protecting them from phishing attacks is extremely important. In our research, we are discussing Three-Factor Authentications for preventing Phishing attacks. In the first authentication after entering a username, the user needs to select few grids of an image which they have received via OTP. In the second authentication, the user will receive a security question which they gave at the time of registration and have to enter the answer for it. In the third authentication, the user's password will be split into two parts. One part of the password will be provided by the bank and the other half will be provided by the user.**

***Keywords*— Phishing Attacks, OTP, Banking Security, IM Services.**

I. INTRODUCTION

Nowadays, every sector works online and crimes are one of the major concern amongst all the sector. Seizures will interrupt into the system base moreover obtaining the data required on produce vulnerability to the systems. We need to secure all the information from the intruders. Attacks can be represented by two forms, i) Quiet Attack and ii) Quick Attack. Phishing is a quiet attack(as per [1]). Phishing is an online tricky exercise where the objective of a phisher is to hijack a victim's raw data, such as online funding account details, identifications or credit card data, therefore, taking money from the people. The link to the infected website is carried out in phishing emails. Phishing email guides the user to share their confidential data. The site then hacks those data that the user has entered. In general, a phished email is sent to a huge number of users (as per [2]). The phisher then counts the number of peoples who have seen that email and shared their data. It is extremely hard to find that we are really operating on a genuine site or a phished site. Brand spoofing or carding are also known as Phishing.

As per the statistics of Anti-Phishing Working Group (APWG) in the period of December2015, the universal phishing websites recognized was 630,494 and the prime brace countries in entertaining phishing sites were Belize, a country in Central America with 81.3% and the United States of America with 76.8% (as per [3]).

Because of this consequence, researchers are trying to miniaturize the chances of vulnerabilities. Banking Security includes safekeeping of private resources from hackers. Normally, authentication deals with the username and password, but owing to increasing risks of hackers these existing text passwords, OTP will not provide sufficient privacy. With the increase in threats, Millions and Millions of money have lost in recent years. To protect the resources against unauthorized and illegal interfaces, authentication is very much needed (as per [4]). Today, not only text keys are used for passwords, images are also used. In a genuine halfway password ensures our privacy, setting our sensitive matters more guarded. This paper is an individual study of images splitting into grids, text password splits as passwords and implementation of a remarkably protected method involving three-factor authentication system. Therefore, to block phishing attacks, I believe that it would be better to develop more levels of authentication.

II. PROPOSED SYSTEM

This suggested solution has a pair of method: a login method and a registration method. I initially begin by introducing participants and theories used.

There are totally four participants. They are a website, an Instant Messaging(IM), the user and the phisher. As we hold a subsequent way to grant the OTP, we first assume the original channel is secure or not. This theory is reasonable as most of the browsers performs the SSL etiquette to encrypt HTTP transaction. Performing of the authentication assistance, we have to assume that the website has joined more than two IM Channels and should use the channels to interact with the users. Furthermost, the user should install anyone of the IM client which is supported by the website. Getting the IM record is pretty easy, and I assume that customer will already have the IM channel accounts. The Instant Messaging assistance doesn't charge, the payment for registering a common public channels is free for the bank and for the user. The user need not install an IM client as most of the Operating System has built-in clients e.g., "Microsoft's Windows Messenger"(as per [5]) and "Apple's iChat in Mac OS X" (as per [6]). Many of the IM clients

automatically signs in, therefore, with a clear setting, a user will join an IM client seamlessly the customer goes online. I think that the IM assistance providers are knowledgeable that their assistance are capable of passing OTPs.

When it comes to a secondary channel, there are many that are available in the market which can deliver OTP, for example, emails, SMS, and Instant Message Service. As per my survey, I consider that an IM assistance is the excellent third-party channel for my system. In extension to addressing messages in real-time, before-mentioned services are relatively universal and free of cost. Despite its security as it is not that secure, with decent form and configuration, it can be a better tool for addressing OTPs. The foundation for IM service is available on the internet. The program can be downloaded and obtained by the user without paying even a single penny. Consequently, to make use of before-mentioned assistance, a site requires to organize an identity administration database and route an IM program to send OTP.

A. Motivation

The motive following the proposed solution is very simple. In my research work, I propose that user can get into their banking accounts securely by three levels of verification out of which the first two levels will be reliable on OTPs which would be addressed via a secure secondary communication channel. The customer information in server should match a user's data with its identical name on another channel. When a customer wants to enter into his account, the server will grant an OTP to the customer. After receiving the message, the user can perform their associated task for that OTP sent to them before the OTP expires. The proposed system will provide three factors of security. A crime will only get cleared if the intruder identifies (1) the customer's nickname; (2) the identification of third-party from which the customer gets OTP; and (3) the key performed to enter third-party(as per [2]). These compulsions elaborate the phishing crime methods.

Most of the active phishing sites are intended to capture the user's login alias and passwords. As per the survey in the year 2009(as per [7]), there are about 70% of sites who steals user's login names and passwords. The phisher will log into the phished account as soon as he retrieves valid username and password of a user and by logging in, the phisher will retrieve further valid informations. As phishers target the user account alias and keys, a fundamental step to miniaturize the aggregate of before-mentioned initiatives is by validating a user with three level of filters. Off these three filters, the first filter would hold an picture burst into frameworks. The second filter would hold security question and the third filter would hold the password. In below section, it is defined more deeply.

B. First Level of Authentication

Usually, many of the banking websites ask for user's username and password to authenticate the user which makes the phisher easily crack into the user's account. In my research work, I apply three-factor for authenticating a user into his/her account. The first factor for authenticating user would hold an image. That picture would signify burst frameworks or grids. Those frameworks or grids would be in the form of a matrix with MxN, where M would be rows of the picture and N would be the columns of the picture. The picture would split to 4x4 matrix grids. Considering 4x4 matrix grids as minimum, we also set maximum grid for the image to be 8x8 matrix grid(as per [13]). After entering the username, the user will be shown an image with these matrix grids. The user will receive an One-Time Password through a secondary channel. The OTP will request the user to select on few matrix grids of that image(as per [14]). On perfectly selecting on those grids(as received in the OTP from the bank through the secondary channel), the user will be taken for further verification.

C. Second Level of Authentication

On successfully completing the first level of authentication, the user will further take for the second verification. In the second verification process, after selecting the grids, the used will be shown a plain text box where the user needs to answer the secret question received to him/her through a secondary channel. The question that would be asked to the user through a secondary channel is the same secret question that the user has given to the bank at the time of registration. Generally, secret questions are offered by the website, but here in my solution, the secret questions will be given by the user itself. So that the phisher should be left out with no idea what the question would be(as per [10]).

D. Third Level of Authentication

After completing two levels of authentication, the user is now shown a text box, where he needs to type in his/her password to successfully login to his/her account. Entering the password is a bit tricky.

At the time of registration, the user gives the password. The password needs to match few criteria which include a combination of alphabets, numbers, and special characters, and the password should be even characters and with a minimum of 8 characters. After the user has given the password, it is divided into two parts. One part of the password is given to the user and the another part of the password is given to the bank server. User's text password is split into two. For instance, if the password is "mohammedmudassir" it is split into two and only "mohammed" will be given by the user and the submit button will be clicked, The website should display the other half of the password to the user. If that half of the password is correct, then the user confirms that the URL what he have approached is correct. [Note: Just for easier representation I have provided an easier password, it would be difficult. for example, if the password is a134abc1, only a134 is entered by the user and abc1 should be displayed to the user in the web application from the bank server].

E. Registration Process

Normally, the enrolment method to a site comprises the below steps. First, the customer must pick a universal nickname, then choose a pass key and give in all the mandatory sections. The user is also requested to give at least one way to communicate (an email or phone number). After performing all the mandatory fields for Bank registration, the customer is now requested to give their IM details for the Bank to send OTP at the time of logging in. The site should show all the IM assistance that the bank accepts to send OTP to the user. After the user has selected any one out of the list provided by the bank, then the user is taken to the IM registration for completing the enrolment process. While registering for the IM, if anything goes wrong then both the IM enrolment operation and the general registration operation will fail. If the customer remains to register their IM, then the site demands for two parts of IM authentication details. The first

would be IM record that will be performed for obtaining OTP which the bank will send to the customer through the IM. The second part of authentication would be the secret question as discussed in section 2.3. Use of these Security questions will surely enhance the privacy of the customer's record.

As the customer inputs IM data, the site the needs to authenticate the legality of the customer's IM record. To prepare that, it transfers customer a authentication page which contains a CAPTCHA test. This blocks the authentication method from being harmed by robots. After this step, the site needs to carry the customer-provided IM record information to their contact and transfers a confirmation information for further checking. If the customer successfully clears the CAPTCHA test, then a sequence of transactions takes place within the Bank, the IM assistance, and the user. A page with validation is transferred to the customer from the IM. The page includes the username of the IM record that is being performed by the Bank site. if in case, the customer's account is fresh to the Bank, then the customer will be requested for a confirmation for adding their account into website's contact list. This ensures that the bank site will always transfer the OTP. This step can be skipped if the user already has any of the accounts supported by the bank for sending OTP. After successfully approving the details of the user from the bank with the IM service, the website then sends an OTP from the designed IM service. The message received will contain OTP. The customer registration process will be validated. Now, this account can be performed for receiving authentication messages when the user wishes to login to his/her account.

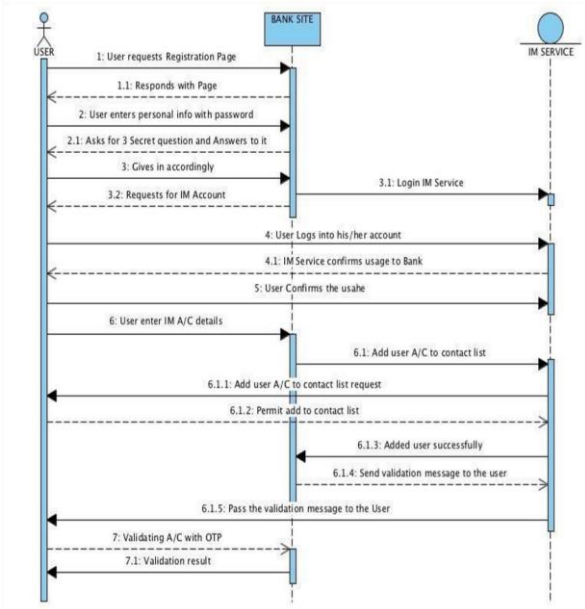

Fig 1. Registration Process

F. Login Process

After the customer enrolled, the customer now log in with the OTP designated by the Bank site. I believe that the Bank Website would have logged into their IM service. The login method comprises of few steps, they are shown below. First, the user needs to log into his/her IM account for receiving OTP from the bank website. Few of the IM clients starts up and logs in automatically, and so I think that this step can be accomplished in the background. Then, the customer begins the exact login method by visiting Bank's Website. In the website, the user is given a text box where the user enters his/her username. After entering the username, the bank authenticates the username and if the username is valid then an image with MXN matrix grids is shown to the user. The matrix grids will be of any size between 4x4 to 8x8. The user then receives an OTP from the Bank through the IM service. In the OTP, the user is requested to select on particular grid or few grids of the image shown to him. As the user selects those grids (as per [8]), the Bank then checks whether the user has selected correct grids or not. If the grids selected by the user is correct, then the user will be shown a text box where the user needs to give the answer for a security question. The security question will be any one of the questions that the user has given to the bank at the time of registration. The security question will be sent by the Bank through a secondary channel that is an IM service. After receiving the security question, the user need to give the answer for that particular question in the text box provided. The answer what the user types in the text box is displayed in a form of bullets. This will prevent any eavesdropper watching you from behind. After typing the answer the user clicks on submit button. If the answer what the user gave matches with the original answer, then the user will be authenticated for final authentication that would be typing his/her password. Since the password is divided into two parts. One part of the password is entered by the user and the another part is given to the Bank's Server. After the user types in his part of password, the bank server should display the another half of the password. If that half of the password is correct, then the user confirms that the URL what he/she have approached is correct. As we use OTP for both login method and registration method, the lifetime of the passwords should be restricted. If the user types an fallacious OTP more than x times or in some cases, a transferred OTP has not been used in y seconds, then the website will nullify the OTP and terminate the process. The user should have to begin the process once again. The objective of this solution is to authenticate the user into their Banking account securely which is through blocking the Internet Protocol (IP) address from which there are more amount of failed attempts(as per [12]). This will help reduce Password Phishing activities.

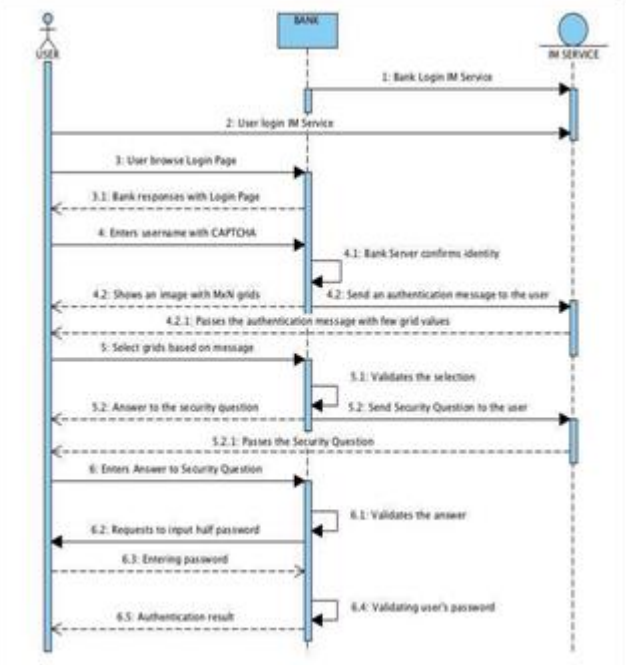

Fig 2. Login Process

III. STABILITY INVESTIGATION

In this division, we analyse the robustness and flaws of the stated system in phases of protection and examine potential enhancements.

A. Negotiating the Stated System

The robustness of the system before mentioned myths in private relations among triple elements and the point that it is challenging to negotiate the elements. The elements are the customer's Bank record, the Bank's IM record, and the customer's IM record. We are considering IM service more because the bank sends OTP to users with the help of these reliable IM services. Henceforth, to negotiate the above-proposed solution, the criminal should know that what are the elements that are associated with each other and then the target the elements subsequently.

B. Authentication in an Untrustworthy location

Suppose the user is not using his/her laptop and needs to log into their Bank account in an untrustworthy location, preferably an internet cafe's openly shared machine. In my research work, I've also thought of these possible situations. This solution is also suitable for these types of situations. Moreover, to help the login method, the user should have another trusted internet supporting device like a smartphone. In this scenario, the user needs to log in his/her IM service first and then continue with the OTP login data. The expected OTP will still be sent to IM record that is recorded with the Bank record. Since the user can access their IM from a trusted device, the user can follow the message received to them and then can log into their Bank account even in an untrustworthy environment. Few IM services permit users to direct the IM to their personal device via SMS when they are not connected to the internet. However, the user receives his/her authentication message even if they are offline.

CONCLUSIONS

The intention of password phishing attack is to hijack user's private and very important information which includes the username of any account along with a password. Despite the technology has grown so far, there are various methods by applying with which we can easily detect phishing act and safeguard customers from criminals, it is not that easy to recognize all the phished websites. In this theory, by applying three levels of filters for both the user and the bank, we can reduce the amount of possible phishing attacks. OTPs are transferred to the user in a universal yet in a safe manner, making it much secure and confidential and also reducing manin-the-middle attack. Therefore, any number of Banking website or any other sector can also take benefit of the before mentioned solution, that is proposed solution. If the bank installs an IM bot at the Bank's server, then they can also reduce the cost of deployment. This will also improve the possibility of the proposed solution. A possible disadvantage of this solution would be IM accounts, as they will become the primary targets for the intruders. Moreover, it is very simple to find out phished exercises with already available methods. This will be possible if the attacker attacks few targets of a small number of websites. Hence, this disadvantage is not a big issue. When the user passes three levels of verification, the number of password phishing activities can be miniaturized. .

REFERENCES

[1] V. Suganya "A Review on Phishing Attacks and Various Anti Phishing Techniques" International Journal of Computer Applications (0975 – 8887) Volume 139 – No.1, April 2016.

[2] Chun-Ying Huang "Using one-time passwords to prevent password phishing attacks" Journal of Network and Computer Applications 34 (2011) 1292–1301.

[3] Phishing Activity Trends Report – APWG.

[4] S.Iswarya Lakshmi "A Four Level Authentication To Bring 100% Web Security By Ensuring Only Genuine Authenticated Web Servers and Users Are Involved In Transactions like Banking, Removing Web Threats ".

[5] Microsoft Corporation. Discover windows messenger, 2009a. [online] /http:// www.microsoft.com/windowsxp/using/windowsmessenger/getstarted/discover.mspxS.

[6] Apple, Inc.. Apple—Mac OS X Leopard— Features—iChat, 2009. [online] /http://www. apple.com/macosx/features/ichat.htmlS.

[7] PhishTank. PhishTank: join the fight against phishing, 2009. [online] /http:// www.phishtank.com/S. URL: /http://www.phishtank.com/S.

[8] Ibrahim Furkan Ince "DESIGNING CAPTCHA ALGORITHM: SPLITTING AND ROTATING THE IMAGES AGAINST OCRs " Third 2008 International Conference on Convergence and Hybrid Information Technology.

[9] David A. Baldwin "The concept of security* " Review of International Studies (1997), 23, 5-26.

[10] Google Security Blog-New Research for security questions. URL:https://security.googleblog.com/2015/05/newresearch-some-tough-questions-for.html.

[11] Naor M. Verification of a human in the loop or identification via the turing test, July 1996. [online] /http://eprints.kfupm.edu.sa/75319/1/7531 9.pdfS.

[12] J. Jayavasanthi Mabel "RESISTING PASSWORD BASED SYSTEMS FROM ONLINE GUESSING ATTACKS" International Conference on Information Systems and Computing (ICISC-2013), INDIA.

[13] AbdulRasheed.Sk "DEFENSES AGAINST LARGE SCALE ONLINE PASSWORD GUESSING ATTACKS BY USING PERSUASIVE CLICK POINTS " [IJESAT] [International Journal of Engineering Science & Advanced Technology] volume-3, Issue-3, 188-193.

[14] Ruchi Kumari " An Image Based Authentication Using Multi-Level Security System " IJESC- Research article, June 2014 issue.