TWO FACTOR AUTHENTICATION FOR REDUCING PHISHING ATTACKS

Nivetha R[1]
Assistant Professor (CS),
Department of Computer Science,
M.M.E.S Women's Arts and Science College,
Melvishram, Vellore

Ramya G[2]
Student MCA,
Department of Computer Application,
VIT University,
Vellore

Abstract

In recent days internet has been used efficiently in almost all the fields and it has grown to a vast extent. Mostly business sectors are preferring to go online for user's convenience as it saves a lot of time and can be easily accessible. For example, Banking Sectors, Online-Shopping, etc,. As the technology grows, we see the negative side in the form of phisher. Phishing is a crime and an activity of stealing user's personal and confidential data. Personal data might be the user's username and password of their account or may be their credit card's information. Our objective is to prevent phishers from hacking the user's personal data. Normally, every online Business sector has a username and password which is not that secured. In our research work, we suggest to make the authentication secured by introducing Two-Factor Authentication. These authentication mechanism will detect and prevent phishing attacks simultaneously and the solution will authenticate both the user and the website in real-time. To get rid of phishers we split images into two parts as first level of authentication and the second level of authentication hold the secret question sent to the user from the Website through a reliable secondary channel.

Keywords: Phishing attacks, Authentication, Bank security.

1. Introduction

Phishing has been increasing dramatically nowadays. The mechanism of a phishing is to grab innocent people's login details, preferably a login detail holds the 'username' and 'password' to enter into their databases. This crime comes into tradition when the intruder sends a false information through a mail. [1] The intruder sends that false information, not to a single person, but they send it to a great number of internet users. That information they send to the user has a fake designed link and these links take the user to their website which is intended to steal customer's data as they use it along the side. Nowadays, intruders create fake banking website with the help of "Phishing Kits" available in the market. As the report published in June 2006, there is about 9255 universal phishing sites, as phishing is growing rapidly. We are unaware of its growth that how much it increases every year. Our aim is to reduce phishing crime in today's world. Web Security involves the protection of confidential resources from hackers. [2] Usually authentication deals with the alias name and keys. Billions and Billions of money are lost in the recent years due the increasing threats.

Authentication plays an important role in protecting resources against unauthorized and illegal interferences. Passwords just don't deals with text keys but also with the images. [7] [8] Eventually, our password guarantees our privacy, placing our sensitive information more secured. This paper is a unique study of images splits, text password splits as passwords and implementation of an extremely secured system applying 2-factor security consisting of

1. Algorithm to Randomize the Split colored pixel of an image, which will be different to each user and falls under the topic Visual Cryptography. [9]

2. Sending Security questions to the user with the help of a third-party communication channel.[10]

Our system of 2-level authentication is briefly explained module by module.

2. Proposed System

When it comes to any online services, we see two of the common process, no matter what the site is, it will definitely a login process and a registration process. The user of those online services is not allowed to access any of the content without having an account. So an account is a needed to have an access on all of their facilities. The user first needs to register for that website service and the needs to get into that account to browse and utilize that facility. There four individuals involved in our theory. They are I. Phisher, II. User, III. Instant Messaging Assistance and IV. Banking site. When talking about the secondary channel, there are many communication channels that serve for delivering messages to the users. For example Electronic messages, SMS and preferably an IM Assistance. We think that IM service will suits better for our system. We are using a third-party communication system to deliver OTP to the user and so we have to make sure that it is securely protected or not. This thought is very much essential as nowadays most of the web browsers perform the SSL set of rules to encrypt Hyper-Text Transfer Protocol transition. Since we are using a third-party communication system, we imagine that the bank has interactions with many of the third-party communication systems and should make usage of that IM assistance make interactions with their customers. Basically, an IM account is free of cost. Any user can create any number of IM accounts. The user need not pay even a single dollar for creating an account. Some of the popular IMs are "iChat by Apple", "Windows Messenger by Microsoft", "Yahoo messenger" etc,.

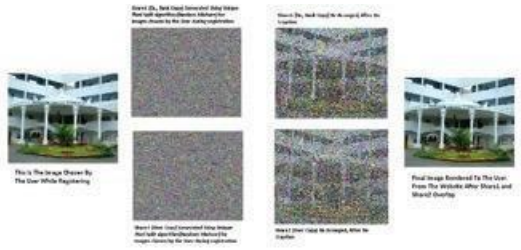
2.1 Motivation

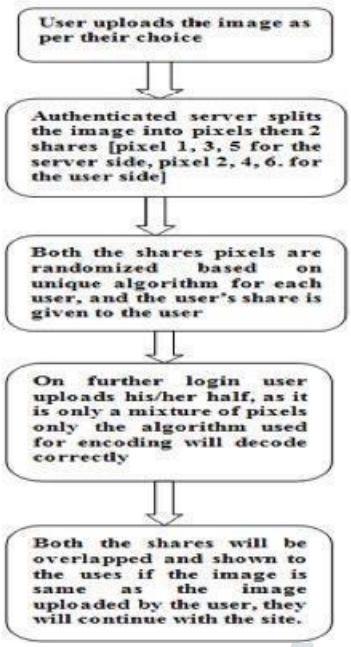
Phishing activities are usually intended to grab user's data which is the login ID and the passwords that they use to login to their databases. [3] As per our survey, there are about 70% of sites that are designed to steal customer's name and a key to login into their account. The intruder will access the victim's account as soon as they get the login credentials. [4] The fundamental goal is to reduce the phishing attacks and so we are introducing two-level authentication for secure logging in. Out of those two levels, the first would have an image whose pixels would be divided into many pixels and then combined together to authenticate the user and the second level would hold a security question for authenticating the site. In the below section, these concepts are elaborately defined in detail.

2.2 First Level of Authentication

Navigating to the right website is the first challenge. To solve the problem, an algorithm to randomize the Split colored pixel, unique for each user falling under the topic Visual Cryptography is used. Let's see this in detail. While registering for the website, the user is asked to upload an image. For example I selected a random picture. This image will be split into two halves [Pixel 1, 3, 5... with the server and Pixels 2, 4, 6 … with the user]. Then both the image share's pixels are re arranged based on any algorithm which is unique for each user. The encrypted image file is given to the user. When the user enters the site for the second time he/she will have to upload their share first. As the decryption algorithm is known only by the Original Site, it will rearrange the pixels and render the merged image to the user. If the User feels it is same as the Image provided by them, they will continue with the site, else they will drop off from the fake website.

Fig. 1. Image chosen by the user while registering



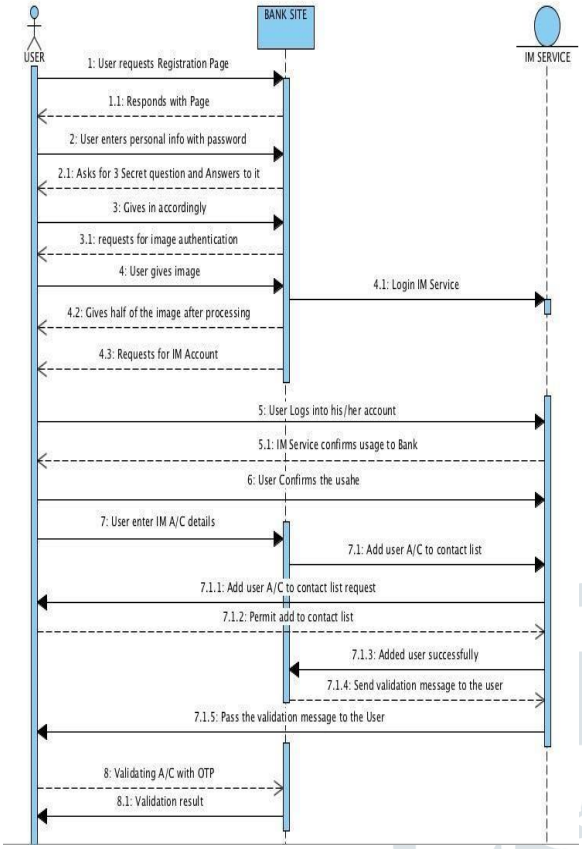


2.3 Second Level of Authentication

To authenticate the user, the bank requests IM to send any of the security question which was already given by the user while registering with bank. IM ask the security question to the user. If user answer the security question correctly, then IM sends an acknowledge to the bank, confirming the user is a authorized person. Now both the bank website and user is authenticated. Bank website redirects the user, to another page to start the transaction.

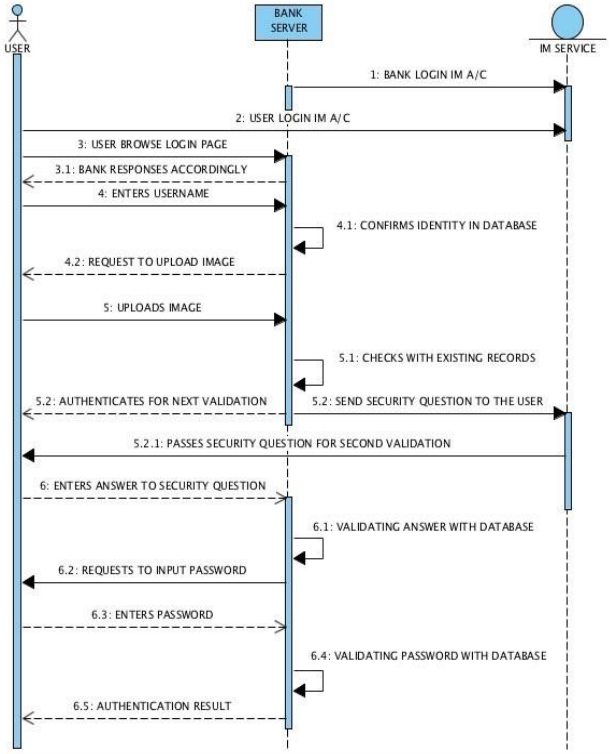
2.4 Registration Process

Initially the bank user have to follow the existing procedures that are normally followed by the bank. That is user has to get the user id and password for his account in which he should follow the rules and regulations that are already prescribed by the bank. After creating the user id and password for the user account. Now he have to follow second step in registration process. And in this process we are using new authentication process where we use the user defined image. This user defined image can be of type like gif, jpeg and that can also be in any bit like 8 bit or in 24 bits. In this step initially user should upload the image in website and that image will be randomized using a specialized algorithm. After randomizing the original image, the whole randomized will be sent to the bank database where it can be used at that time of login process to authenticate the user whether uploaded part by the user is correct or not. And now this randomized image will be divided into two parts and the first part will be sent to the bank database with user id and with the user account details. And the next part of the randomized image will sent to user where the user have to upload this part at that time of login process. And now we are in third process where we have to choose some IM services in which we have to give some security questions for the user authentication where this question will be asked at that time of login process. Initially in this process we have to choose one IM service from the list of IM services. And after choosing the IM service we have to give some security questions and answers where this questions will be asked to user at that time of login process and the user must give the same answer that he already gave at that time of registration process Here the bank only know which IM service has been choose by the user. And bank will doesn't have any idea about the security questions. And at the time login process bank will redirect the user to the IM service and where all the questions will be asked to the user. And after finishing this process that IM service will again redirect the user to the bank website.



2.5 Login Process

The user has to follow the set of criteria given by the bank website to login. The user is checking whether it is "original bank site" or "phisher site". Now search for the bank website then the user enter the username in the bank website. The bank website will check whether the username given by the user is present in bank database or not. If it is not present in the database it will stops the login process. Otherwise continue with the login process i.e the user has to upload his half image given by the bank at time of registration. The image uploaded by the user and also the half image that already exists in bank database are merged together. Then the fetched image is send back to the user, user will compare with his original image if it same the user confirms it is not a phishers website and continues with the login process. Now the user can identify that it is an authorized bank site and validates the user with another step of authentication where bank request the IM to ask the security question to the user. The IM assistance will ask the user a question through a secondary communication channel, that is the IM itself. The user needs to give answer to that same question asked to him through a secondary channel. If the answer matches the question's answer that was submitted to the bank at the time of registration, then the user will be authenticated. If the answer validates, then the user is asked to enter the password of the account and then they can access their account safely.



3. Defence Investigation

In this subdivision, we will discuss and examine our system's strength and weakness for its security purpose and also for its chances of enhancements.

3.1 Shared Confirmation

There is a protection characteristic which facilitates the Bank Server which is the website to confirm a consumer and vice versa. That protection characteristic is Shared Confirmation feature. In our system, the bank server confirms the identity of a customer by applying two levels of validation and confirmation in order to avoid phishing crime in both the bank server side and also with the customer side. Those two levels of authentication include uploading an image followed by the security question and then giving the password as general. In this system, what we have designed is universal as the OTP which is delivered to the customer is not know to anyone except the customer

itself. The customer confirms the banking site at the beginning itself when he/she receives the confirmation from the third-party channel. We think that the Instant Messaging Assistance will stop all the messages from unknown senders; hence only the exact assistance will be able to send all confirmation messages. Any unreliable response to the security question, or invalid security question will terminate the authentication of the bank website.

3.2 Validation in an Untrustworthy Environment

In our proposed system, we make use of images, as well as IM assistance. We carry that randomized image in our laptops with us to log into our accounts safely. But in some scenarios, we may come across a situation where we don't carry our personal devices to secure log in. [5] In such cases, we have to access our accounts in an unreliable location. e.g., accessing our private banking accounts with the help of a publicly joint computers in internet cafes. In order to facilitate the accurate and secure way of logging into our accounts, a customer should have to carry another internet based device with internet connection. The customer should also have that image uploaded to any of the online cloud computing for a truly accessible communication. [6] As the customer types in their alias then he is requested to upload that image. The customer then gets that image from the cloud storage where he uploaded that image and then uploads that image to the bank site for confirming its identity. The OTP which is required to send the security question to the user for further validation of the user. Some IM assistance also provides redirection of instant messages onto customer's registered mobile number via SMS when they are not connected to the Network. Thus, customers can also access their bank accounts in an untrustworthy location.

4. Conclusion

Increasing security approach applied to this system makes it more secured. So these 2-factors will definitely help in avoiding all the major security breaches. This system is surely a little time consuming approach as the client has to pass through the 2-security levels. But it will be as a heavenly gift for the areas where high confidential secrecy is primary purpose and time complexity and all other are secondary.

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/new-research-some-tough-questions-for.html.