Enhancing Security of User Accounts against Phishing using Multi Stage Authentication

Venus Kour[1], Kamal Kumar Sharma[2], Sharad Chouhan[3]

[1]Student, M. Tech, E-Max group of Institutions, Ambala
[2]Professor, Dept. of ECE, E-Max group of Institutions, Ambala
[3]Assistant Professor, Deptt. of CS, E-Max group of Institutions, Ambala

Abstract: In a transition from physical world to online world, more and more people are getting hooked to Web Applications for their operations be it online banking or ecommerce or online ticketing. But in this online world thousands of people across the world fall prey to Hackers and expose their online credentials to theses hackers, who in turn gain access to the users social or financial information and can exploit this information for their gains and users loss.

With the advent of online Applications User focus has shifted from Phishing is one of the hacking techniques used by hackers by the intention of gathering the personal details and credentials of unsuspected users. Phishing websites are duplicate websites that looks similar in appearance but different in destination. The unsuspected users post their data thinking that these websites come from trusted financial institutions and their data is eventually captured by Hackers. Hence there is a need for efficient mechanism for developing Phishing Proof Websites. Our Application applies a Multi Stage Authentication Mechanism with a concept of Visual Image Identification and One Time Password Mechanism all combined together to prevent Hacking through Phishing

Keywords: Phishing, Multi Stage Authentication, One Time Password, Hacking, Phishing attacks, Phishing Website.

I. INTRODUCTION

Since the last few years the number of users using the internet has increased rapidly, so this makes the developers to create more suitable methods to access information on the internet securely. As internet services grow, the defenseless websites will become the targets for the hackers or criminals who will try to attack. Security is the main problem in password-protected websites, because it uses simple authentication mechanisms which are easily exploited by hackers by creating a similar mock website and gather user Data through Phishing. We use a Muti stage authentication mechanism strategy that will help websites keep phishing attacks at bay by combining a number of techniques.

II. PHISHING

Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. Phishing scams have been receiving extensive press coverage because such attacks have been escalating in number and sophistication. Phishing is not limited to the most common attack in which targets are sent spoofed (and often poorly spelt) messages imploring them to divulge private information. Instead and as recently documented both in academic and criminal aspects, phishing is a multi-faceted techno-social problem for which there is no known single silver bullet. As a result of these insights, an increasing number of researchers and practitioners are attempting to quantify risks and degrees of vulnerabilities in order to understand where to focus protective measures.

Phishing Attack Stages

Phishing attacks involve several stages:

- The attacker obtains E-mail addresses for the intended victims. These could be guessed or obtained from a variety of sources.
- The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action.
- The attacker sends the E-mail to the intended victims in a way that appears legitimate and obscures the true source.
- Depending on the content of the E-mail, the recipient opens a malicious attachment, completes a form, or visits a web site.
- The attacker harvests the victim's sensitive information and may exploit it in the future.

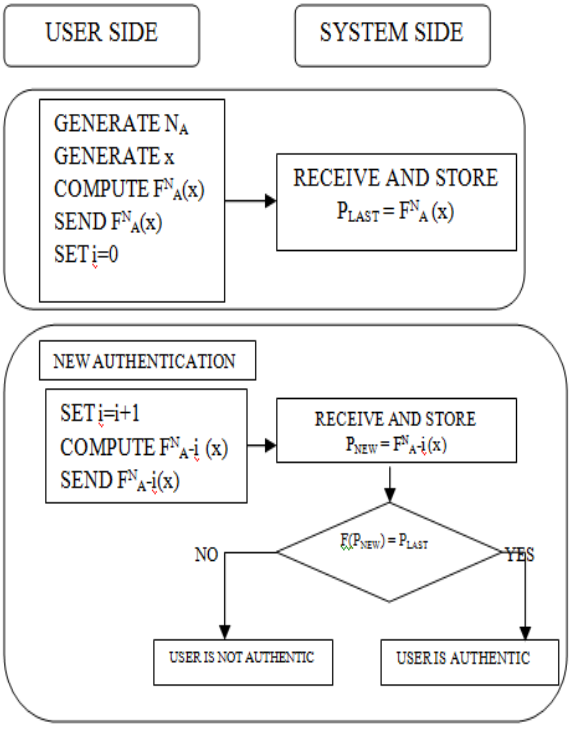
III. MULTI-STAGE AUTHENTICATION

Multi-Stage Authentication (MSA) is a method of user access control where the user credentials are entered by

the user in Steps and on different Pages. We make the system so complex so that it is difficult for hackers to create phishing page for the same. Our System doesn't have a single page for user authentication, the user has to pass through a number of steps to enter their credentials. The First Step Involves entering UserName Only while in other sites user has to enter username as well as password which makes it easier for hackers to create a page similar to the original and when presented to user who unsuspectingly enters his all credentials username as well as password into the Phishing Page and his account gets Comporomised. In our approach we have the just the username in the first step. After proceeding to the second step we have a Inmage Verification system along with a OTP, once user has authenticated these two then only their password will be asked for other wise user is restricted at that point only. No if a hacked had to create a Phishing environment it would be very difficult for them to replicate all these steps as these steps involve information which is not available with User.

IV. ONE TIME PASSWORD

One Time Password is a authentication mechanism in which a Password is Generated on the go and delivered to the user every time they attempt to log in to the system.
Lamport (1981) has proposed a functional one-time Password scheme in which secrets are stored only on the user side and intercepting a password sent from user to the system would not lead to an impersonation.
The authentication process is suggested in Figure 1.



Lamport's authentication is based on computing the sequence {x, F(x),F1(x),F 2 (x),..., F NA (x)} on the user side, where x is an arbitrary value chosen by the user and kept secret, NA is the number of authentications to be performed and may be also chose by the user, F is a known one way function (this means that by giving x it is easy to compute F(x) but by giving F(x) it is infeasible to compute x).[4]
At the beginning the system must know F NA (x) and then when the user needs to authenticate for the first time to the system (i =1) he will present F NA−1 (x) as the first one-time password. At the ith authentication the user will prove its identity by sending F NA−i (x) and the system will simply verify this by computing F(F NA−i (x)) and also checking that F(F NA−i (x)) = F NA−i+1(x) , where F NA−i+1 (x) is the previous authentic one time password. This scheme may also be viewed as a challenge-response protocol where the challenge is defined by the position of the password in the password sequence (Menezes et al., 1996, page 396).

V. IMAGE VERIFICATION

Another Authentication Factor an Image Verification Mechanism is added into the application. Image Seal is an Image that has been uploaded by user from his computer at the time of registration. Now at the time of login the same image along with two more images is shown to the user, from them he has to select the image uploaded by him. This serves two purposes one is adding an alternative authentication mechanism and most importantly that it prevents phishing attacks as the Hacker who has created Phishing Website wont be able to serve the same image that was uploaded by the User.

VI. LITERATURE SURVEYED

Mohit G. et. al. discusses the different ethics in the cyber crime including the mechanisms of phishing and vishing The ethics centers and program devoted to business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have sprung up. These centres are designed to examine the implications of moral principles and practices in all spheres of human activity on our lives. Cyber crime is emerging as a serious threat. World Wide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. This article is an attempt to provide a glimpse on cyber crime in India. [1].
Vipul G. et. al. discusses the importance of One Time Password and how it can help in reducing Hacking attempts. In the Paper The One Time Password System is described as described which is secure against eavesdropping and server database compromise at the same time. Traditionally, these properties have proven to be difficult to satisfy at the same time and only one previous scheme i.e. Lamport Hashes also called S/KEY one time password system has claimed to achieve that.

Lamport hashes however have a limitation that they are computationally intensive for the client and the number of times a client may login before the system should be re-initialized is small. We address these limitations to come up with a new scheme called the N/R one time password system.

The basic idea is have the server aid the client computation by inserting 'breakpoints' in the hash chains. Client computational requirements are dramatically reduced without any increase in the server computational requirements and the number of times a client may login before the system has to be re-initialized is also increased significantly. The system is particularly suited for mobile and constrained devices having limited computational power. [2]

T. Lakshmi Praveena et. al provides an insight of Multi Factor Authentication System. It discusses Online information maintenance through cloud applications allows users to store, manage, control and share their information with other users as well as Cloud service providers. There have been serious privacy concerns about outsourcing user information to cloud servers. But also due to an increasing number of cloud data security incidents happened in recent years. Proposed system is a privacy-preserving system using Attribute based Multifactor Authentication. Proposed system provides privacy to users data with efficient authentication and store them on cloud servers such that servers do not have access to sensitive user information. Meanwhile users can maintain full control over access to their uploaded files and data, by assigning ?ne-grained, attribute-based access privileges to selected files and data, while diferent users can have access to diferent parts of the System. This application allows clients to set privileges to different users to access their data. [3]

Jyoti Chhikara et. al. defines Phishing as a con game that scammers use to collect personal information from unsuspecting users. The false e-mails often look surprisingly legitimate and even the Web pages where users are asked to enter their information may look real. Phishing is similar to fishing in a lake, but instead of trying to capture fish, phishers attempt to steal personal information. This paper gives brief information about phishing, its attacks, steps that users can take to safeguard their confidential information. This paper also shows a survey conducted by netcraft on phishing. [6]

VII. CONCLUSION

The Paper mainly emphases on implementing a multi stage authentication system to prevent hackers from hacking into user accounts via phishing. The implementation follows a set of rules that username and password are not to be authenticated at same step but at different steps along with combining other Authentication mechanisms like Visual Image Verification and OTP Password.

VIII. REFRENCES

[1]. Mohit Goyal, "ETHICS AND CYBER CRIME IN INDIA", IJEMR Vol 2(1) 2012

[2]. Vipul Goyal, Ajith Abraham, Sugata Sanyal and Sang Yong Han, "The N/R One Time Password System" TIFR

[3]. Lakshmi T Praveena, V Ramachandran and Ch. Rupa. Article: Attribute based Multifactor Authentication for Cloud Applications. International Journal of Computer Applications 80(17):37-40, October 2013.

[4]. L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM 24.11 (November 1981), pp 770-772.

[5]. Dr.D.S.Rao, Gurleen Kour, "One Time Password Security through Cryptography For Mobile Banking", IJCTA, Vol 2 (5), 2011.

[6]. Jyoti Chhikara, Ritu Dahiya, Neha Garg, Monika Ran, "Phishing & Anti-Phishing Techniques: Case Study", IJARCSSE Volume 3, Issue 5, 2011.

