ISSN:0975-9646

Intelligent Approach toward Anti-Phishing using Two Factor Authentication

Hardik Desai Deepak Gupta Noopur Pandey

Department of Computer Engineering,
Thakur College of Engineering and Technology, Mumbai University, India

Abstract-*Phishing is an attempt to commit fraud via social engineering. The impact is the breach of information security through the compromise of confidential data. Customers can access their banking accounts from anywhere in the world using their login ID and password. However, the use of password does not provide adequate protection against Internet fraud such as phishing. Phishing exploits this vulnerability to fraudulently acquire sensitive personal information, such as username, passwords and/or credit card details. Usually this is achieved by masquerading as a trustworthy person or business with an apparently legitimate request for information. In this paper we have proposed a new approach named as IAPC which includes captcha followed by two factor authentication. Two factor authentication is carried out using steganography mechanism to hide the password inside an image. MD5 and DES (Data Encryption Standard) encryption techniques are used to encrypt the hidden password.*

Keywords: IAPC, MD5, DES, CAIN, TLD.

I. INTRODUCTION

Phishing has become the fastest growing scam on the Internet, and some are even beginning to target businesses rather than individual users. The goal of most phishing attacks is to obtain personal information from an individual which can be used later by the illegitimate user for their benefit purpose. Security is the prevention of, or protection against the access to information by unauthorized recipients and unauthorized destruction or alteration of that information.

The key requirements of any system to be secure are the following: *Confidentiality, Authenticity, Integrity, and Non-Repudiation* that constitutes the acronym "CAIN". Confidentiality is the concealment of information or resources so that the information only be accessible for reading by authorized parties, Authenticity is the identification and assurance of the origin of information, Integrity is necessary to keep the computer system asset unmodified without authentication and Non-repudiation associates the identity of the originator with the transaction in a non-deniable way which means originator of communications cannot deny the transaction later. Illegitimate users exploit one or more of these aspects to carry out their attacks.

Figure 1. Unique Phishing Site Detected January – June 2011

The number of unique phishing websites detected by APWG during H1, 2011 fluctuated by over 10,000 websites within the half year. Reaching the highest point in March with 38,173, the half year low was in June with 28,148. The half yearly high in March was down more than 32 percent from the record high of 56,362 recorded in August 2009 [1].

II. BACKGROUND STUDY

Phishing sites were categorized based upon the domains they leveraged. The most targeted industry sectors during 1st half 2011 are shown in figure 3 [2].

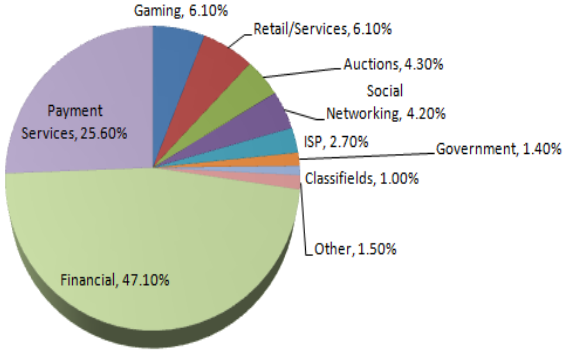

Figure 2. Overall Statistics for phishing attacks

Financial Services continued to be the most targeted industry sector in the first half of 2011. Payment Services which last eclipsed Financial Services in 2010 remained the second highest industry sector for targeted attacks. There are many types of network attack through which the attacker can gain access to the communication and can steal the important information of the authorized user.

Government-hosted phishing sites were even used to attack other governments for example the website of the UK government, Directgov, was targeted in 14 of these phishing attacks. All of the phishing content used in these attacks was hosted on Peruvian government domains, but has since been removed [4].

Table 1. Phishing sites hosted on government Top-level domains.

Government TLD	Country	New phishing sites in July 2011
gob.pe	Peru	69
gov.br	Brazil	12
go.th	Thailand	11
gob.mx	Mexico	9
gov.cn	China	9
gov.ar	Argentina	6
gov.za	South Africa	6
gov.pk	Pakistan	3
gov.ec	Ecuador	3
gov.tr	Turkey	3

Anti-Phishing Working Group (APWG) founded in 2003, is focused on eliminating the identity theft and frauds that result from the growing problem of phishing, crimeware, and email spoofing. APWG tracks the number of unique phishing websites. APWG additionally tracks crimeware instances (unique software applications as determined by MD5 hash of the crimeware sample) as well as unique sites that are distributing crimeware (typically via browser drive-by exploits) [1].

	Jan.	Feb.	March	April	May	June
Number of unique phishing email reports received by APWG from consumers	23,535	25,018	26,402	20,908	22,195	22,273
Number of unique phishing web sites detected	29,815	31,544	38,173	33,008	35,213	28,148
Number of brands hijacked by phishing campaigns	339	335	313	333	331	310
Country hosting the most phishing websites	USA	USA	USA	USA	USA	USA
Contain some form of target name in URL	69.82%	74.97%	72.38%	72.16%	78.82%	76.55%
No hostname; just IP address	3.18%	3.31%	3.38%	4.15%	4.14%	3.38%
Percentage of sites not using port 80	0.59%	0.52%	1.11%	0.78%	0.44%	0.45%

Figure 3. Statistical highlights for 1st half, 2011

III. TYPES OF PHISHING ATTACKS

Nowadays, the nature of attacks is more active rather than passive. Previously, the threats were all passive such as password guessing, dumpster diving and shoulder surfing. Here are some of the techniques used by the attackers today:

A. Trojan Attack:

The attacker installed a Trojan, such as key logger program, on a user's computer. When users log into their bank's website, the information keyed in during that session will be captured and sent to the attacker. Here, the attacker uses the Trojan as an agent to piggyback information from the user's computer to his backyard and make any fraudulent transactions whenever he wants.

B. Man-in-the-Middle Attack:

Here, the attacker creates a fake website and catches the attention of users to that website. Once successful, instead of going to the designated website, users do not realize that they actually go to the fraudster's website. The information keyed in during that session will be captured and the fraudsters can make their own transactions at the same time.

Other network attacks which are used by the attacker for retrieving the information of the user are sniffing: password grabbing, Brute Force: password attempts, Buffer Overflows: httpd, ftpd, rpc/dcom, Spoofing Attacks: forging IP/MAC/Etc and Masquerading. Phishing works as an indirect attack on cyber world [3].

IV. CURRENT SCENARIO

In the current scenario, when the end user wants to access his confidential information online by logging into his bank account, the person enters information like username, password, and other credentials. But quite often, this information can be captured by attackers using phishing techniques (for instance, a phishing website can collect the login information the user enters and redirect him to the original site).

A technique to redirect users from real websites to the fraudulent websites by using malware/spyware, typically through DNS poisoning, DNS hijacking or 'hosts' file manipulation.

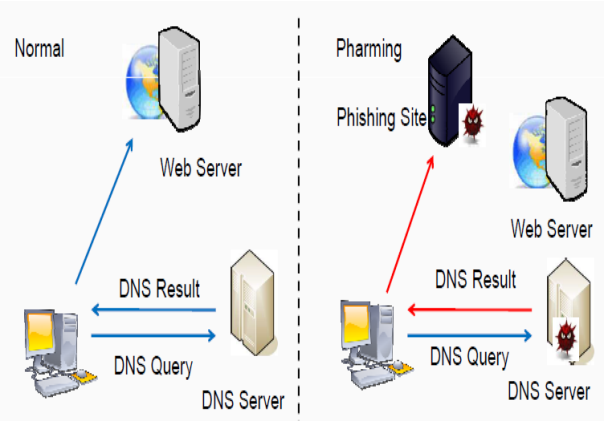

Figure 4. Current Scenario

V. PROPOSED METHODOLOGY

Every sensitive data that are transferred on the web are capable of being getting attack. Detecting and identifying phishing websites in real-time, particularly for e-banking is really a complex and dynamic problem involving many factors and criteria. Also many phishing detection and prevention tools are not 100% secure. So we are proposing a new methodology to detect the phishing website. Our methodology is based on the Anti-Phishing Image Captcha validation scheme. It prevents username, password and other confidential information from the phishing websites.

IAPC approach is divided into two phases:

A. Registration Phase

B. Login Phase

A. Registration Phase

In this methodology, the user needs to fill his/her personal information along with the primary password which will be used at the login time. During registration automatic captcha will be generated which will let user know the website is genuine. After the user has been registered a randomly generated unique customer id will be generated by the system which will be used for login in into the account for using transaction or other functionality of the banking website.

B. Login Phase

When user logs in by entering the customer id (generated after the successful registration) along with the primary password, a secondary password hidden in the image is generated and send to the user's electronic mailing address provided at the time of registration.

This secondary password is then hidden into an image using steganography mechanism. The most important goal of security enhancement using data hiding in image is to hide messages within the image so the intended receiver of the image get the data of his interest in the form of the image so even if this image fall in wrong hand chances are less that person receiving the image get to know that some data is hidden in the image. This kind of technology is very useful in case of increasing security of the secure system. Through hiding a secret message inside the Image, a simple image is taken as carrier to carry the data to be hidden in it. Once Image is obtained, data that needs to be hidden is taken from user and is placed between the data bytes of actual image such that receiver of the image may consider it as normal image but when supply this image to decoder, can extract the hidden message within it in its entirety.

For secure communication between the user and the confidential website the secondary password will be one time password and also the password stored in the database will be deleted once used.

Here IAPC (Intelligent Authentication Phishing Control) plays three roles for security, which are as follows:

- ✓ ***It verifies whether the website is a genuine/secure website or a phishing website.***
  If the website is a phishing website then in that situation the secondary password which is used as an anti-phishing code will not generated and user would not be able to access the account. So it can be easily verified by the specific user for any website that the website is a phishing website (attacker website) or a genuine website.
- ✓ ***It verifies whether the user accessing the website is a human user or a machine based user (provides hacking security).***
  The captcha generated during the registration time will only be readable by human users alone and not by machine users. Only human users accessing the website can read the captcha and reproduce it in text form.
- ✓ ***It prevents intruders' attacks on the user's account.***
  Even if the intruder extracts the secondary password from the image he/she would not be able to identify the password since the password will be encrypted using two well known encryption techniques MD5 and DES. And also without knowing how the secondary password has been generated, he cannot decrypt the password and hence cannot enter the password and log in into the given account.

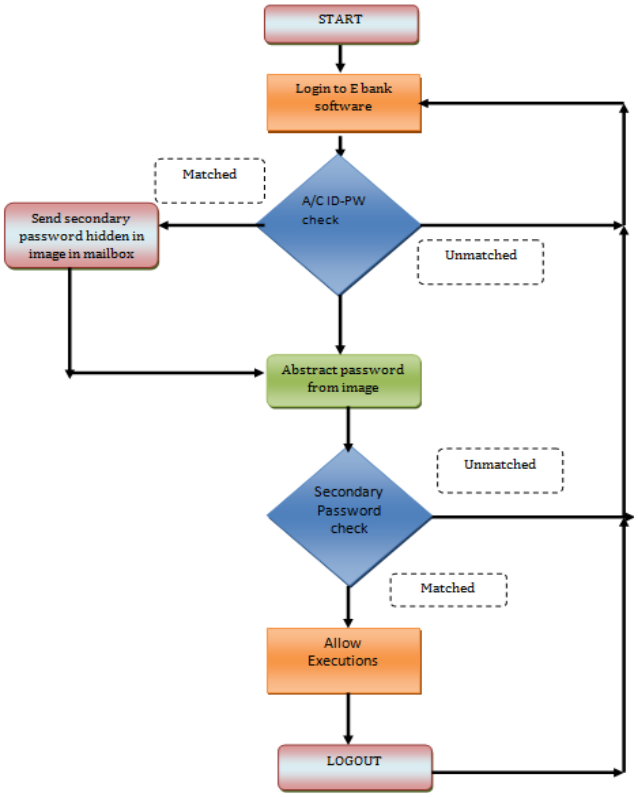

Figure 5. Flow chart shows the process carried out during login phase.

VI. IMPLEMENTATION OF PROPOSED METHODOLOGY

We have implemented Secure Banking Layer web-based application along with demo banking website for demonstrating our proposed methodology. We have used Core Java, MS Access / SQL Server, JSP, Servlet, Java MAIL API, LOG4J framework for logging, Tomcat as web container in implementing the methodology. We have also

learnt the concepts of Core Java and Servlet from the reference [5][6].

Our Two factor authentication acts like a three tier architecture where Image captcha acts as a middleware between the login phase and user account.

- The user will be login in into the E-banking account using the valid customer id and the primary password once the user has been registered.
- After the successful login of first phase, user need to go through the middleware authentication i.e. Image captcha for becoming an authorized user. The Image encoded with the secondary password will be send to the user electronic mailing account.
- So for accessing the account the user needs to download the image into his/her system and provide the path were the image has been downloaded for example C:\Users\Downloads\ABC.png.
- After entering the valid path the user will be authenticated and he/she will be allowed to access the account and its functionality.

Figure 6. Registration screen showing the unique generate Customer Id.

Figure 7. Login screen for accessing the account.

Figure 8. User authentication screen.

Figure 9. Screen showing user account after successful login through Image Captcha Authentication technique.

VII. CONCLUSION

The providers of Internet banking services must be more responsive security requirements. While there is no doubt that Internet banking transaction should have layered protection against security threats, the providers should approach security considerations as part of their service offerings.

Currently, there are no formal processes being put in place to determine the level of security provided by these service providers and to what minimum standards they should be.

Local financial institutions should consider the above-mentioned recommendations to ensure confidentiality of customer information.

VIII. FUTURE WORK

A system is not complete as the requirements change from time to time. It is always possible to incorporate changing requirements with minimum efforts. The system is planned to cater to new features and implementation expansion scenarios. The system is developed having foresight of future.

Additional Requirement: Three Factor Authentication

However, for a better security, a three factor authentication process should be considered. The third authentication factor is the use of biometric such as iris or thumbprint recognition. This ascertains who one is, biologically. This method of authentication has been introduced by the Employee Provident Fund (EPF) for it members, but is limited to getting the latest statements of a member.

With a three-factor authentication a more secure method can be implemented - a password to ascertain what one knows, a token (smartcard) to ascertain what one has, and biometric recognition (for example fingerprint or thumbprint) to ascertain who one biologically is.

As such, if passwords have been compromised, fraudsters need to get through another two levels of authentication to access a customers account. This would be difficult, if not totally impossible.

IX. ACKNOWLEDGEMENT

The authors would like to thank Mr. Adesh Devdas Nayak of Thakur College of Engineering & Technology, Mumbai for the support provided for this work.

X. REFERENCE

[1] Ronnie Manning, "Phishing Activity Trends Report", AWPG, January-June, 2011.
[2] Symantec Security Response Anti-Fraud Team, The State of Phishing A Monthly Report – January 2010.
[3] Ahmad Nasir Zin ABCP and Zahri Yunos ABCP
National ICT Security and Emergency Response Centre (NISER), "HOW TO MAKE ONLINE BANKING SECURE", *The Star InTech*, 21 April, 2005.
[4] LulzSec and Wikileaks, "Netcraft's Anti-phishing Internet Research Report", July, 2011.
[5] Complete Reference Java2, Fourth Edition.
[6] Head First Servlets and JSP by Bryan Basham, Kathy Sierra, Bert Bates.

XI. BIOGRAPHY OF AUTHORS

Mr. Deepak Gupta, Mr. Hardik Desai and Ms. Noopur Pandey are all final year students in Computer Engineering Department at Thakur College of Engineering and Technology, Mumbai University. They have keen interest towards System Security and Web-based app-development. So they have decided to build a Secure Banking Layer web-based application under the watchful guidance of ***Dr. Rekha Sharma*** and ***Mrs. Vidyadhari Singh.*** Both the guides have motivated us throughout the development of the application. We have considered all the feasibility factors and are quite motivated towards the development of the application.