Anti-phishing and SQL Injection Prevention System for E-Bank Website Security

Mr.Desale Akash [1], Miss.Ghogare Monika [2], Miss.Kakade Rajashri [3], Miss.Kolhe Seema[4], Prof.kahate S. A.[5]

[1]Student,Computer,SPCOE, Pune,Maharashtra, India,
[2]Student,Computer,SPCOE, Pune, Maharashtra, India,
[3]Student,Computer,SPCOE, Pune,Maharashtra, India,
[4]Student,Computer,SPCOE, Pune,Maharashtra, India,
[5] Assi.Professor, Computer,SPCOE, Pune,Maharashtra, India,

ABSTRACT

Phishing is an internet fraud that acquires a users credentials by deceptions. It includes theft of password, credit card number, bank account details, and other confidential information. Aim to develop Best security system against Phishing and SQL Injection attacks. People purchase products online and make payment through e-banking.Develop system to detect the e-banking phishing website our system uses an effective classification data mining algorithm. The e-banking phishing website can be detected based on some important characteristics like URL and Domain Identity, and security and encryption criteria in the final phishing detection rate. The e-banking phishing website can be detected based on some important characteristics like URL and Domain Identity and security. This application can be used by many E-commerce enterprises in order to make the whole transaction process secure.Also SQL injection attack is the most common attack in websites in these days. Some malicious codes get injected to the database by unauthorized users and get the access of the database due to lack of input validation. Our Aim to presents the techniques for detection and prevention of SQL injection attack.

Keyword: - *Phishing, network proxy, blacklists, anti-Phishing countermeasures, e-commerce security, online banking security.*

1. INTRODUCTION

Phishing attacks have become a serious problem for users of online banking and e-commerce websites. In this paper develop Best security system against Phishing and SQL Injection attacks.People purchase products online and make payment through e-banking. There are many E-banking phishing websites. Now, develop system to detect the e-banking phishing website our system uses an effective classification data mining algorithm. The e-banking phishing website can be detected based on some important characteristics like URL and Domain Identity, and security and encryption criteria in the final phishing detection rate. The e-banking phishing website can be detected based on some important characteristics like URL and Domain Identity, and security. Once user makes transaction through online when he makes payment through e-banking website our system will use data mining algorithm to detect whether the e-banking website is phishing website or not. This application can be used by many E-commerce enterprises in order to make the whole transaction process secure.

Seeking sensitive user data in the form of online banking user_id and passwords or credit card information, which may then be used by 'phishers' for their own personal gain is the primary objective of the phishing e-mails.

Also, add Best feature for website security name as SQL injection attack prevention. We going to use SQL injection blocker for enhance website security.

I. PHISHING ATTACK PROCEDURE AND PREVENTION METHODS

A. THE PROCEDURE OF PHISHING ATTACKS

1) Phishers set up a counterfeited Web site which looks exactly like the legitimate Web site, including setting up the web server, applying the DNS server name, and creating the web pages similar to the destination Website, etc.

2) Send large amount of spoofed e-mails to target users in the name of those legitimate companies and organizations, trying to convince the potential victims to visit their Web sites.

3) Receivers receive the e-mail, open it, and click the spoofed hyperlink in the e-mail, and input the required information.

4) Phishers steal the personal information and perform their fraud such as transferring money from the victims account.

B. APPROACHES TO PREVENT PHISHING ATTACKS

There are several (technical or non-technical) ways to prevent phishing attacks:
1) Educate users to understand how phishing attacks work and be alert when phishing-a like e-mails are received.

2) Use legal methods to punish phishing attackers.

3) Use technical methods to stop phishing attackers. In this research paper, only focus on the third one. Technically, if we can cut off one or several of the steps that needed by a phishing attack, then successfully prevent that attack. In what follows, briefly review these approaches.

2. LITERATURE SURVEY:

1. Token Based Security for Prevention of Phishing Attack at Client Side

A database of tokens (hash codes) of legitimate web sites' URLs is stored on the client machine. When a user enters a site address in the browser, the system computes its integrity code and matches it with the stored integrity code (token). For the validation of the proposed system, it has been compared with the existing 'white list' based anti phishing method in terms of false positive and false negative metrics.

2. Anti Phishing for Mid-Range Mobile Phones

E-commerce trade has experienced the largest number of cyber crimes that includes various types of security attacks. Phishing attack is the one most common among these all, as the mobile banking is getting popular, hence protecting the mobile users from phishing attacks is very important; particularly mid-range mobile users, because these users are easy target of attackers as mid-range mobile phones do not support feature like anti-virus or anti-phishing tool.

3. Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm

Phishing is a new type of network attack where the attacker creates a replica of an existing Web page to fool users (e.g., by using specially designed e-mails or instant messages) into submitting personal, financial, or password data to what they think is their service provides' Web site. In this research paper, we proposed a new end-host based anti-phishing algorithm, which we call Link Guard, by utilizing the generic characteristics of the hyperlinks in phishing attacks. These characteristics are derived by analyzing the phishing data archive provided by the Anti-Phishing Working Group (APWG). Because it is based on the generic characteristics of phishing attacks, Link Guard can detect not only known but also unknown phishing attacks. We have implemented Link Guard in Windows XP.

3. OBJECTIVE:

• To enhance cyber security by Anti- Phishing system.

• To study SQL Injection system in cyber forensics.

• To develop Website Security System. Examine the major Functionality of today including, URL Filtering, IP DNS Filtering, SQL Injection Prevention.

4. PROBLEM STATEMENT:

We develop a project for E-Bank Website Security using Anti-Phishing and SQL injection Prevention. Our system is effective to detect and prevent both known and unknown phishing attacks with minimal false negatives. Also used for detection and prevention of SQL injection attack.

5. SYSTEM ARCHITECTURE:

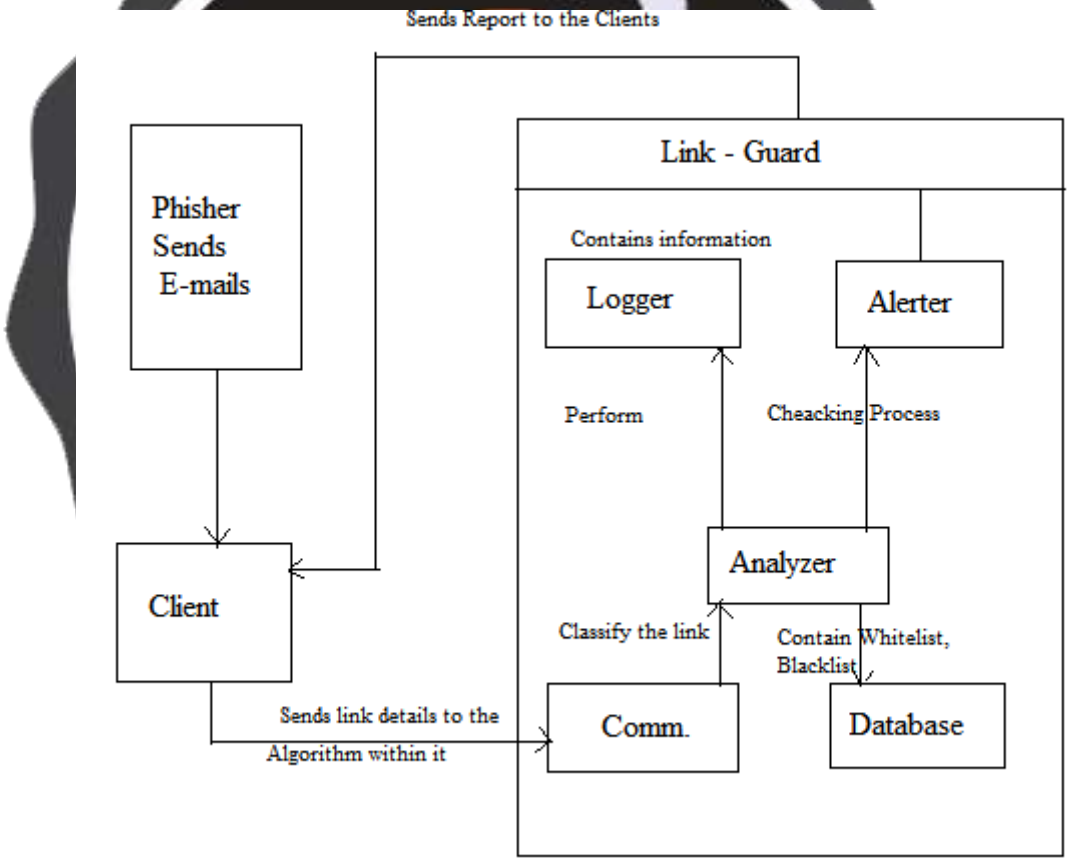

Fig. 1. System Architecture

1) Install a BHO (browser helper object) for IE to monitor user input URLs.
2) Install an event hook with the Set WiEventHook provided by the Windows operating system to collect relevant information.
3) Retrieve sender's e-mail address from Outlook.
4) Analyze and filter the received windows and browser events passed by the BHO and the hook, and pass the analyzed data to the Link Guard executive. Link Guard is the key component of the implementation. It is a stand-alone windows program with GUI (graphic user interface). Analyzer, Alerted, Logger, Comma, and Database. The functionalities of these 5 parts are given below:

Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm.

Comm: Communicate with the whook.dll of all of the monitored processes, collect data related to user input from other processes (e.g. IE, outlook, Firefox, etc.), and send these data to the Analyzer, it can also send commands (such as block the phishing sites) from the Link Guard executive to whook.dll. The communication between the Link Guard process and other processes is realized by the shared memory mechanism provided by the operating system.

Database: Store the whitelist, blacklist, and the user input URLs.

Analyzer: It is the key component of LinkGuard, which implements the LinkGuard algorithm; it uses data provided by Comm and Database, and sends the results to the Alert and Logger modules.

Alerter: When receiving warning messages from Analyzer, it shows the related information to alert the users and send back the reactions of the user back to the Analyzer.

Logger: Archive the history information, such as use revents, alert information, for future use. After implemented the LinkGuard system, we have designed experiments to verify the effectiveness of our algorithm. Since we are interested in testing Link Guard's ability to detect unknown phishing attacks, we set both whitelist and black list to empty in our experiment..

5.1 Existing System:-

1) Users username & password Hacked Easily
2) Difficult to classify Real or Fake Login Page
3) IP and DNS Spoofing Vulnerable
4) SQL Injection Vulnerable system

5.2 Proposed System:-

1) Classify and Notify website Phishing Existence
2) Prevention IP &DNS spoofing Attack
3) Sql Injection Attack Preventer

6. ALGORITHM:

LINK GUARD ALGORITHM:

Link Guard works by analyzing the differences between the visual link and the actual link. It also calculates the similarities of a URI with a known trusted site. The algorithm is illustrated in Figure. The following terminologies are used in the algorithm.

Description of the Link Guard algorithm.. The Link Guard algorithm works as follows. In its main routine Link Guard, it first extracts the DNS names from the actual and the visual links. It then compares the actual and visual DNS names, if these names are not the same, then it is phishing of category 1. If dotted decimal IP address is directly used in actual DNS, it is then a possible phishing attack of category 2 . Delay the discussion of how to handle possible phishing attacks later. If the actual link or the visual link is encoded.

We first decode the links, then recursively call Link Guard to return a result. When there is no destination information (DNS name or dotted IP address) in the visual link (category 5), Link Guard calls Analyze DNS to analyze the actual DNS. Link Guard therefore handles all the 5 categories of phishing attacks. Analyzes and the related subroutines are depicted in Fig.2. In Analyze DNS, if the actual dns name is contained in the blacklist, then we are sure that it is a phishing attack Similarly, if the actual DNS is contained in the whitelist, it is therefore not a phishing attack. If the actual DNS is not contained in either whitelist or blacklist, Pattern Matching is then invoked.

1. Make Whitelist and Blacklist Database to store IP and DNS.
2. User Request for particular Website using Domain and IP.

3. Antiphishing system Extract actual IP Address from DNS.
4. Automatically start Link Guard Algorithm Checking Protocols.
    i. Compare Requested Domain is Whitelist or Blacklist.
    ii. Requested Domain must be HTTPS Protocol.
    iii. Domain must be in www.domain.com/in/net/org or more URL Filtering.
5. If condition satisfy all this things then Requested Page is not Phishing.
6. If condition satisfy < 80% then phishing page found.
7. And project prevent SQL injection attack using Input Validation.

6.1 Advantages:-

- Trusted System For Communication.
- Robust than traditional Anti-phishing system.

7. CONCLUSION

Phishing has becoming a serious network security problem, causing finical loss of billions of dollars to both consumers and e-commerce companies. And perhaps more fundamentally, phishing has made e-commerce distrusted and less attractive to normal consumers. In this paper, we have studied the characteristics of the hyperlinks that were embedded in phishing e-mails. We then designed an anti-phishing algorithm, Link Guard, based on the derived characteristics. Since Phishing Guard is characteristic based, it can not only detect known attacks, but also is effective to the unknown ones. We have implemented Link Guard for Windows XP. Our experiment showed that Link Guard is light-weighted and can detect up to 96unknown phishing attacks in real-time. We believe that Link Guard is not only useful for detecting phishing attacks, but also can shield users from malicious or unsolicited links in Web pages and Instant messages. Our future work includes further extending the Link Guard algorithm, so that it can handle CSS (cross site scripting) attacks.

8. ACKNOWLEDGEMENT

I. I WOULD LIKE TO TAKE THIS OPPORTUNITY TO EXPRESS MY SINCERE GRATITUDE TO MY PROJECT GUIDE & HEAD OF DEPARTMENT PROF. KAHATE S.A. AND CO-GUIDE PROF. KURHE B.S. FOR HIS ENCOURAGEMENT, GUIDANCE, AND INSIGHT THROUGHOUT THE RESEARCH AND IN THE PREPARATION OF THIS DISSERTATION, HE TRULY EXEMPLIFIES THE MERIT OF TECHNICAL EXCELLENCE AND ACADEMIC WISDOM. HIS EXTENSIVE KNOWLEDGE, SERIOUS RESEARCH ATTITUDE AND ENCOURAGEMENT WERE EXTREMELY VALUABLE TO ME. I ALSO APPRECIATE NOT ONLY FOR HIS PROFESSIONAL, TIMELY AND VALUABLE ADVICES, BUT ALSO FOR HIS CONTINUOUS SCHEDULED FOLLOW UP AND VALUABLE COMMENTS DURING MY RESEARCH WORK. I SHOULD ALSO LIKE TO ACKNOWLEDGE THE CONTRIBUTION OF MY PRINCIPAL DR. G.U.KHARAT

9. REFERENCES

[1] S. Philippsohn, “Trends In Cybercrime — An Overview Of Current Financial Crimes On The Internet”, in *Computers & Security*, 20 (1), 2001 pp. 53-69.

[2] Cyber Source, “9th Annual Online Fraud Report”, Edition: 2008 [online]. Available: http://www.cybersource.com, last access on 20/3/2007.

[3] J. S. Downs, M. B. Holbrook and L. F. Cranor, “Decision strategies and susceptibility to phishing”. Proc. the 2nd symposium on usable privacy and security. New York, USA: ACM Press, 2006, pp. 79 – 90.

[4] M. Chandrasekaran, R. Chinchani and S. Upadhyaya, "PHONEY: Mimicking User Response to Detect Phishing Attacks". Proc. International Symposium on a World of Wireless, Mobile and Multimedia Networks. Washington DC: IEEE Computer Society, 2006, pp. 668-672.

[5] A. Litan, "The War on Phishing Is Far From Over", Report: 2009 [online]. Gartner Group. Available: http://www.gartner.com/DisplayDocument?ref=g_search&id=927921, last access on 25 June 2009.

[6] S. A. Robila and J. W. Ragucci, "Don't be a Phish: Steps in User Education". Proc.1th annual SIGCSE conference on innovation and technology in computer science education. New York: ACM Press, 2006, pp. 237 – 241.

[7] Symantec, "Mitigating Online Fraud: Customer Confidence, Brand Protection, and Loss Minimization", 2004 report [online]. Available: http:// www.antiphishing.org/sponsors_technical_papers/ Symantec_online_fraud.pdf, last access on 21/3/2007.

[8] A. Alnajim and M. Munro, "Effects of Technical Abilities and Phishing Knowledge on Phishing Websites Detection". Proc. the IASTED International Conference on Software Engineering (SE 2009), Innsbruck, Austria, ACTA Press, 2009, pp. 120-125.

[9] A. Alnajim and M. Munro, "An Anti-Phishing Approach that Uses Training Intervention for Phishing Websites Detection". Proc. 6th IEEE International Conference on Information Technology - New Generations (ITNG). Las Vegas, IEEE Computer Society, 2009, pp. 405-410.

BIOGRAPHIES

	**Mr. Desale Akash** is a student of 7th semester in Department of Computer Science, Sharadchandra Pawar college of Engg, Otur He is working on the project titled Single Sign On Mechanism for Multiple Social Media Sites. This paper is the outcome of the application being developed.
	**Miss.Ghogare Monika** is a student of 7th semester in Department of Computer Science, Sharadchandra Pawar college of Engg,Otur He is working on the project titled Single Sign On Mechanism for Multiple Social Media Sites. This paper is the outcome of the application being developed.

Miss.Kakade Rajashri is a student of 7th semester in Department of Computer Science,Sharadchandra Pawar college of Engg,Otur She is working on the project titled Single Sign On Mechanism for Multiple Social Media Sites.This paper is the outcome of the application being developed.

Miss.Kolhe Seema is a student of 7th semester in Department of Computer Science,Sharadchandra Pawar college of Engg,Otur she is working on the project titled Single Sign On Mechanism for Multiple Social Media Sites.This paper is the outcome of the application being developed.

Assi. Prof. Kahate S. A. B.E. & M.E. Assistant Professor, Department of Computer Engg. Sharadchandra Pawar College Of Engg, Otur, Pune(India)sandip.kahate@gmail.com