Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

On the Mechanism of Detection and Prevention from Phishing attacks by Analyzing the Attacker Behavior

Rimmy Chuchra,
Department of Computer Science and Engineering,
Sri Sai College of Engineering and Technology,
Amritsar, India

Dr. R. K. Seth,
Department of Applied Sciences,
Sri Sai College of Engineering and Technology,
Amritsar, India

Reenuka Gujral, Priyanka Sharma
Department of Computer Science and Engineering,
DAV University, Jalandhar, India

Abstract: The paper focuses on the serious concern regarding major threat of phishing attacks on worldwide financial transactions of any enterprise. These attacks are becoming popular and increasing at a high rate that creates problems for social networking sites and financial websites while using internet banking. In this paper, the behavior of the attacker on the client system or on the server system is analyzed. The two different mechanisms based upon port scanning and rule induction data mining on the online mode techniques has been proposed. The procedure utilizing the proposed mechanisms helps potentially to reduce phishing attacks by analyzing the behavior of attacker during the transmission of data from the starting to end point while an attacker insert a malicious SQL query as an input to perform an unauthorized database operation.

Keywords: Phishing, phishing attack, rule Induction, active attacks, SQL injection.

I. INTRODUCTION

Phishing is significantly growing problem that threatens to impose increasing monetary losses on businesses and to shatter consumer confidence in e-commerce. Phishing is basically web spoofing and a major growing problem. Currently, Internet banking becomes more popular in our society having several benefits such as easy to use, saving transport to the bank and queue time on the counter."Internet banking" is the most attractive channel for theft information by attackers upon the credit card details and bank account passwords etc. Using Phishing attacks, attackers easily perform bank robbery and steal money. Generally, Social Phishing use public gatherable information and lure user to a spoofed website to get their secured information [1] [8]. In our daily life, a number of forged e-mails can be seen that comes from various banking sites to user accounts and holds a hyperlink in the message box [5]. If any user clicks on those links and visits on that specific website, then user Id and password are stolen by the phishers and phishers could use that specific account details (userId and password) for future and then phisher can login to the real rank's website and transfer the victim's money to his own account[7]. In order to avoid phishing attacks, the preference must be given to enter any bank site address manually and avoid direct clicking on the various banking sites addresses. Phishing site cannot display correct counter password i.e. the code generated after entering the userId and before entering password) in spite of other normal websites easily display correct counter password details. In this way, it may be said that it's too hard for unprofessional people to detect or prevent phishing and becomes easy for attackers to get valuable information from legitimate users [6]. In this paper, the behavior of the attacker is analyzed in two phases that described in the paper considering the following attacks on the systems.

a) Attack on the client system.
b) Attack on the server system.

The chances of attacks on the server system such as any banking sites server are more than on a client system. If attack will be done on the client system then only client system will be responsible and similarly if attack is on the server then only server will be the responsible for that attack.

An Attacker first attack on any bank databases by using **"SQL injection"** and steal complete information of user accounts like password and credit card details etc. After stolen these details attacker will behave like phisher for performing phishing attack during the transfer of money online. We will identify phishing attack by using three different mechanisms: "port scanning", "Rule induction data mining technique" and correct counter password method. After identification of the phishing attack we must have to provide prevention from phishing attack by using proposed mechanism which is discussed in this paper. And we can also reduce the chances of attacker by using the virtual keyboard rather than a simple keyboard. This is an alternative method for providing prevention from phishing attacks [2] [3]**.**

II. CONCEPT

In this paper, the behavior of the attacker is analyzed in first step from where attack will be done by the attacker. Considering the attacker's behavior in two phases that may affect client system as well as server system, the concept has been described as follows:

When attacker affects client system: When any attacker directly attacks on the client system, then all requests sending from the client system will be directly send to the attacker system rather than the actual server system. Even on that time client is unaware from such type of client system attack because client receives a message display that "transaction completes successfully". In this case only client system will be responsible for the attack rather than server system.

When attacker affects server system:

Any client that sends request to the server system with full security but server system will be already injected by the attacker then in this case only server will be the responsible. For example, when any user transfers his/her money from one account to another account, then during money transfer any problem occurring from the server side makes the server responsible. Such kind of problem is generally faced by the people when attack is directly done on the server side. Recently in US, a very small amount of money (27 penny) has been stolen from every account, where even the users do not keep in their mind exact bank balance and end result is that attacker get advantage of collecting huge amount of money.

In this way we can say that analysis of the attacker behavior becomes a necessary step to study. The chances of attack will be more in bank server system rather than client system.

During internet banking like online money transfers by ATMs and credit card payments, phishing attacks are being performed. Single phishing attacks can therefore thousands of individual URL'S while leading to essential phishing site.

Description of Procedure: The description of the procedure followed by the attacker is discussed in the following steps:

1. It has been reviewed that through the **"SQL Injection",** attacker uses any bank databases. (In case of **SQL injection attack,** an attacker might insert a malicious SQL query as input to perform an unauthorized database operation).

"SQL Injection" is a hacking technique that is applied on various bank databases which attempts to pass SQL commands through the web application for the execution by backend databases. Such types of attacks allows hackers to view information from the databases and use dynamic script languages including ASP,ASP.NET,PHP,JSP etc.

2. In the second step, after injecting the databases, the attacker performs next "PHISHING ATTACK".

3. In the third step, we must have to identify the phishing attacks by two different methods. These are listed below:

- "PORT SCANNING".
- We can also identify phishing attack online by web robots that are basically web agents by using "Rule Induction data mining technique".

Using "Port Scanning method", we can easily identify the registered IP Addresses and easily check either they are valid or not. If any unknown IP Address or hacker IP Address will come and try to access system data then we will easily detect. This hacker IP Address and other details like type of data will be hacked by the hacker through the network will easily be identified by the "WIRESHARK SOFTWARE" which is generally used by the intrusion detection system using data mining [4].

IF **Condition** Then **Class**.

i.e. - IF Attack Status=Enable then Call=Web Agents.

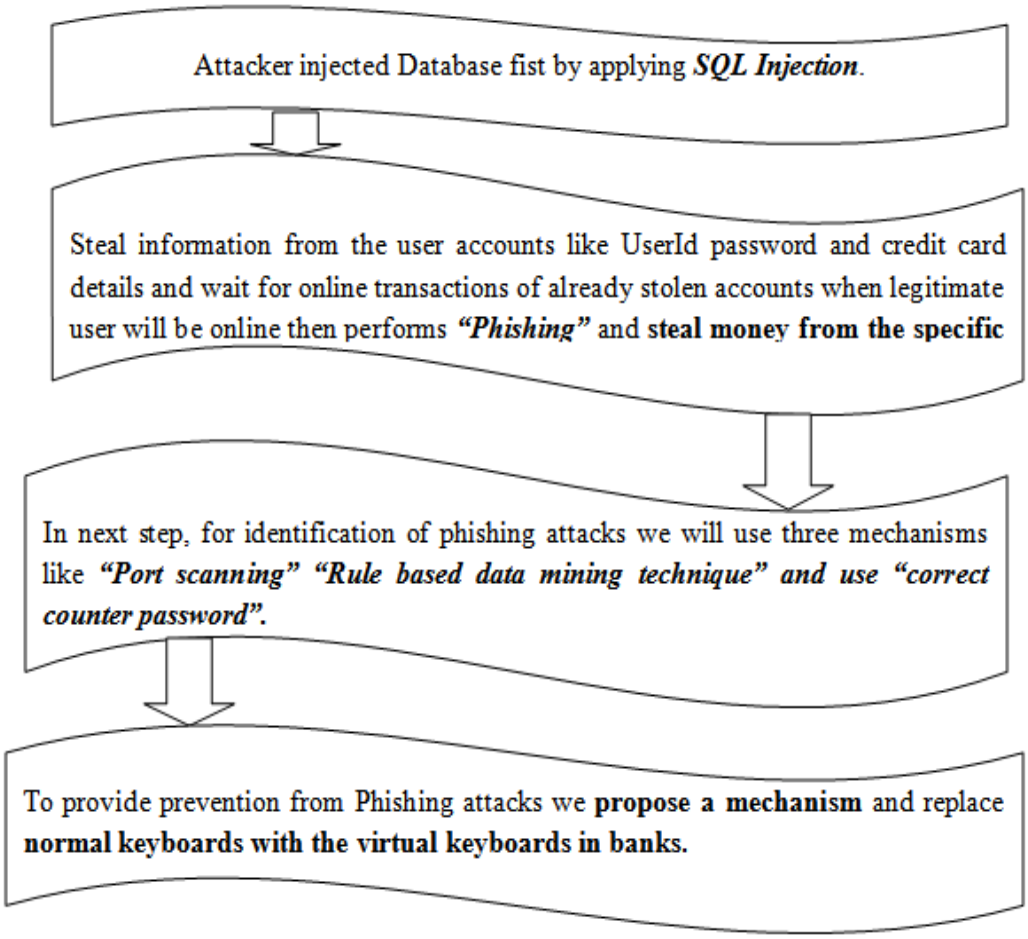

Fig 1: Procedure followed by the attacker.

The ***major purpose to use "Rule induction technique"*** is to achieve the maximum accuracy for getting better results. Rule Induction technique can be implemented as follows:

Table1: Nomenclature used in rule induction method.

WA	Web Agent
AA	Active Attack
OnM	Online Mode
S	Status
E	Enable(shows value is 1)
D	Disable(shows value is 0)
R	Rule

For each Class WA
Initialize to the set of all A2

While Active Attack contains examples in class WA

Create a rule "R" with an empty L.H.S that
Predicts Class WA

Until R is 100% accurate (Or there is no more status to use) do:

For each status "S" not in R & each Mode (Online mode_OnM).

Consider adding the condition (Status_Mode pair) S=M
To the L.H.S of R.

Select S and M in which status of attack is disabling & helps to maximize the rule accuracy & also covering of the Status_Mode Pair.
Add Status=mode to R (rule).

Removed the examples covered by R from all A2.

There is only one **possible case of Status_Mode Pair** which are as follows:-

Case1: Status=Enable, Mode=Online.
Status=Disable, Mode=Online.

Description: When status is enabling and mode is online that indicates data is to be transferred from the source to the destination and when status in disable and mode is again online that indicates there is no data transferred between the source and the destination [4].

4. In the fourth step, we propose a new mechanism which provides prevention from phishing attacks which is discussed as follows:

- If password is copied from the server and saves a copy in the log files created by the system, then create a method or logic that helps to expire UserId and send message to the client, your Id is expired and Sign Up again after contacting concerned nearest bank branch. After that a new UserId will be issued by the bank for the same user. In this case only server will be responsible for attack. In future, next time whenever an attacker will come with same ID then easily can detect the attacker by his/her ID.

- By replacing normal keyboard with the virtual keyboard we can also reduce the chances of the attacker for performing phishing attack.

- It is important to note that with the help of web agent or web robot, we can easily identify the attacker by applying rule based data mining technique during online mode.

III. RESEARCH METHODOLOGY

Description: When any client wants to transfer money from client system to other bank server then he/she must use a proper channel for money transfer that is called "Internet connection". Through internet connection transactions will be completed but every time internet connections are not secure. So, in first step focus on secure connection after that perform any transaction otherwise the possibility to steal the data by the attacker increases.
In the proposed research design, a user wants to transfer money to the bank server through the "virtual private network". During money transfer, when black hat hacker will attack on the server then immediately connection will break and page will be reloaded with the display of warning message on the client system side. Even user requests for reloading the page will always be unsuccessful.

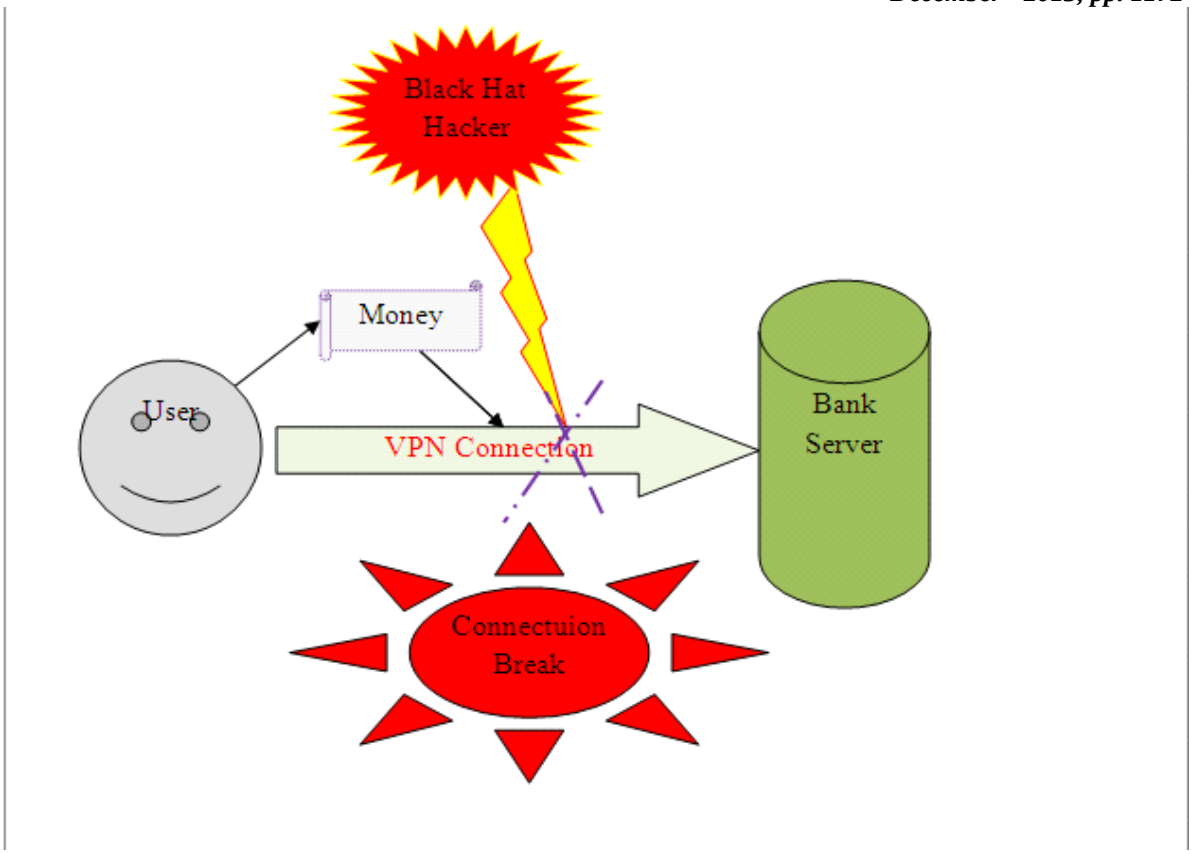

Fig 2: Phishing attack done on bank server.

IV. CONCLUSIONS

In this paper, the behavior of the attacker in two modes has been analyzed on the client system and on the server system. After analyzing the behavior of the attacker, the phishing attacks are identified using three different methods such as port scanning and rule induction data mining technique on online mode and proposed a new mechanism that helps to provide prevention from phishing attacks once password is copied from the server User Id and send message to the client your Id is expired and Sign Up again after contacting concerned nearest bank branch. After that a new User Id will be issued by the bank for the same user. The proposed mechanism may be used to detect and prevent the phishing attacks.

FUTURE SCOPE

"Wire shark" has a lot of scope in future for identifying the phishing attacks. The specific function of this software is to read all live packets captured data i.e. what is exactly going on the network and also helps to display network traffic data. With the utilization of this software, the phishing attacker can easily be identified. The methodology based upon "wire shark" shows the complete working of packet data streams

REFERENCES

[1] Email spoofing From Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/Email_spoofing Accessed: March 11, 2012.

[2] Yi Yan, Su Zhengyuan, Dai Zucheng,"The Database Protection System against SQL Attacks", 2011 IEEE.

[3] Atefeh Tajpour, Suhaimi Ibrahim, Maslin Masrom," SQL Injection Detection and Prevention Techniques", International Journal of Advancements in Computing Technology Volume 3, Number 7, August 2011.

[4] Human robotics interaction with data mining techniques, IJETAE, ISSN (2250-2459), vol.3, Issue2,Feb-2013,pp.99-101.

[5] Normal, K.; Ewards, S.E.V.; Geetha, K.; "Maximizing online security by providing a 3 factor authentication system to counter-attack 'Phishing'", in Proceedings of IEEE- International Conference on Emerging Trends in Robotics and Communication Technologies, 2010.

[6] Mohsen Sharif, Alireza Saberi, Mojtaba Vahidi, and Mohammad Zorufi, A Zero Knowledge Password Proof Mutual Authentication Technique against Real-Time Phishing Attacks, Springer-Verlag Berli Heidelberg 2007.

[7] http://share.pdfonline.com/61ad6805cd564326a8f7695be3635f00/main.htm.

[8] T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer, "Social Phishing", Commun. ACM 50(10), pp. 94-100, October 2007.DOI: 10.1145/1290958.1290968.

