MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 – 6953

SECURING INTERNET BANKING FROM PHISHING ATTACK

Sushant Kamble, Amit Malshikare , Poonam Gargund, Chaitrali Bhagwat
Department of Computer Engineering
Marathwada Mitra Mandals College of Engineering
Pune, India
sushantkamble.comp@mmcoe.edu.in, amitmalshikare.comp@mmcoe.edu.in,
poonamgargund.comp@mmcoe.edu.in, chaitralibhagwat.comp@mmcoe.edu.in

Abstract: *Phishing is now serious threat banking system for user confidential information. Basically, a phisher tricks people into divulging sensitive information by sending fake message to a large no of users at random .Unsuspecting users who follow the instruction message are directed to well-built spoofed web pages and asked to provide sensitive information, which phisher steals causing negative purpose. Security is playing a very important role in field of network communication system and internet .In this project we are discussing how to detect phishing attack in banking system and how to prevent it by using different algorithms like DES(Data Encryption Standard), Image based feature extraction and Link Guard algorithm.*

Keywords: *Cipher Text, Plain text, Encryption, Network security, hyperlink, URL Redirection, Image Extraction.*

1. INTRODUCTION

Phishing is a new word produced from 'fishing',[1] it refers to the act that the attacker allure users to visit a faked Web site by sending them faked e-mails (or instant messages), and stealthily get victim's personal information such as username, password, and national security ID, etc. This information then can be used for future target advertisements or even identity theft attacks (e.g., transfer money from victims' bank account). The frequently used attack method is to send e-mails to potential victims, which seemed to be sent by banks, online organizations, or ISPs. In these e-mails, they will make up some causes, e.g. the password of your credit card had been mis-entered for many times, or they are providing upgrading services, to allure you visit their Web site to confirm or modify your account number and password through the hyperlink provided in the e-mail. If you input the account number and password, the attackers then successfully collect the information at the server

side, and is able to perform their next step actions with that information (e.g., withdraw money out from your account).Phishing itself is not a new concept, but it's increasingly used by phishers to steal user information and perform business crime in recent years.

The common characteristics of the hyperlinks in phishing e-mails. Our analysis identifies that the phishing hyperlinks share one or more characteristics as listed below:

1) The visual link and the actual link are not the same;
2) The attackers often use dotted decimal IP address instead of DNS name;
3) Special tricks are used to encode the hyperlinks maliciously;
4) The attackers often use fake DNS names that are similar (but not identical) with target website.

1.1 Phishing

Basically PHISHING is the process of creating fake web pages and by sending spoofed E-mail to user Phisher steals the confidential information such as usernames, passwords and bank details. Phishing methods can include the following:

1) Internet Banking Phishing
2) Phone Phishing
3) Wi-Fi Hotspots
4) By Using Phone Apps

All these phishing is elaborated in figure as shown in below:

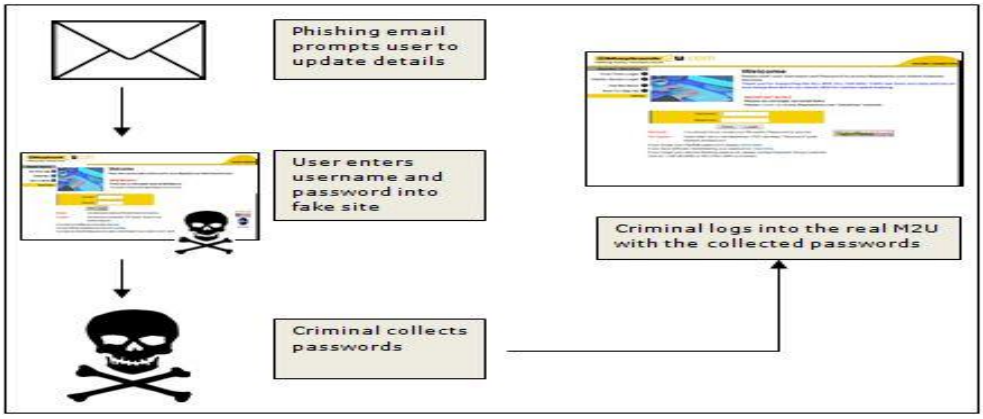

Fig.1: Elaboration of Phishing Attack. [4]

If a phisher wishes to coordinate other attacks, he will evaluate the successes and failures of the completed scam and begin the cycle again. Phishing scams often take advantage of software and security weaknesses on both the client and server sides.

2. RELATED WORK

2.1. Detect and block the phishing Web sites in time [3]: If we can detect the phishing Web sites in time, we then can block the sites and prevent phishing attacks. It's relatively easy to (manually) determine whether a site is a phishing site or not, but it's difficult to find those phishing sites out in time.

2.2. Enhance the security of the web sites [3]: The business Websites such as the Web sites of banks can take new methods to guarantee the security of users' personal information. One method to enhance the security is to use hardware devices. For example, the Barclays bank provides a hand-held card reader to the users. Before shopping in the net, users need to insert their credit card into the card reader, and input their (personal identification number) PIN code, then the card reader will produce a onetime security password, users can perform transactions only after the right password is input.

2.3. Block the phishing e-mails by various spam filters [3]: Phishers generally use e-mails as 'bait' to allure potential victims. SMTP (Simple Mail Transfer Protocol) is the protocol to deliver e-mails in the Internet.

2.4. Install online anti-phishing software in user's computers [3]: Despite all the above efforts, it is still possible for the users to visit the spoofed Web sites. As a last defense, users can install anti-phishing tools in their computers.

The Anti-phishing tools in use today can be divided into two categories:

1) Blacklist
2) white list

3. PROPOSED SCHEME

In the proposed solution, first to process the simple Columnar Transposition with Multiple Rounds (SCTTMR).The plain text massage is first converted into cipher text by using simple Columnar Transposition Technique. To apply this scheme we require matrix or table to perform encryption process and column no which provide security key. Image extraction contains two parts .One is to build site signatures for websites and another is to match web pages against site signatures .features included in site signatures can be classified into two types ,i.e., text- based and image -based features. Link Guard works by analyzing the difference between the visual link and the actual link. It also calculates the similarities of a URI with a known trusted.

3.1. Data Encryption Standard (DES) Algorithm

DES is a block cipher. It encrypts the data in a block of 64 bits. It produces 64 bit cipher text. The key length is 56 bits. Initially the key is consisting of 64 bits. The bit position 8, 16, 24, 32,40,48,56, 64 discarded from the key length [16].

DES is based on two fundamental attributes of cryptography: Substitution (confusion) and transposition (Diffusion).DES consists of 16 steps, each of which called as a Round.

Algorithm:

1) In the first step, the initial 64-bit plain text block is handed over to in Initial Permutation (IP) function.
2) The Initial permutation is performed on plain text.
3) The initial permutation produce two halves of permuted block: Left Plain text (LPT) and Right Plain Text (RPT).

4) Now, each of LPT and RPT goes through 16 rounds of encryption process, each with its own key:
   a. From the 56-bit key, a different 48-bit Sub-key is generated using Key Transformation.
   b. Using the Expansion Permutation, the RPT is expended from 32 bits to 48 bits.
   c. Now, the 48-bit key is XORed with 48-bit RPT and resulting output is given to the next step.
   d. Using the S-box substitution produced the 32-bit from 48-bit.
   e. These 32 bits are permuted using P-Box Permutation.
   f. The P-Box output 32 bits are XORed with the LPT 32 bits.
   g. The results of the XORed 32 bits are become the RPT and old RPT become the LPT.This process is called as Swapping.
   h. Now the RPT again given to the next round and performed the 15 more rounds.
5) After the completion of 16 rounds the Final Permutation performed.

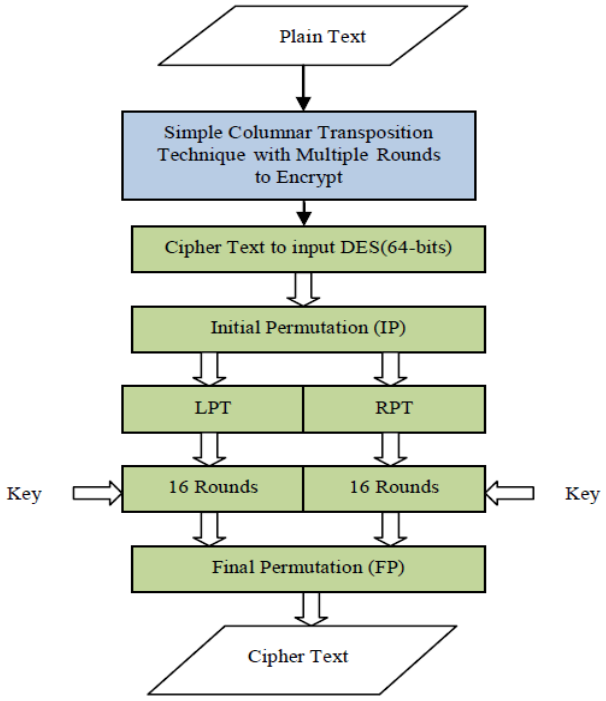

Fig.2: Encryption with Enhanced DES.[4]

3.2. Link Guard Algorithm

A Classification of the hyperlinks in the phishing e-mails. In order to (illegally) collect useful information from potential victims, phishers generally tries to convince the users to click the hyperlink embedded in the phishing e-mail. A hyperlink has a structure as follows.
<a href="URI"> Anchor text <\a>Where ‘URI’ (universal resource identifiers) provides the necessary information needed for the user to access the networked resource and ‘Anchor text’ is the text that will be displayed in user’s Web browser.
In our project we are going to compare the original link i.e. URL with the visited link. If both are matched each other then it is safe for processing the banking functionality else it shows the message that someone is trying to steal your information and it will redirect to the original

web page. Examples of URIs are http://www.google.com, https://www.icbc.com.cn/login.html.

Algorithm:

```
v_dns = GetDNSName (v_link);
a_dns = GetDNSName (a_link);
if ((v_dns and a_dns are not
empty) and (v_dns! = a_dns))
return PHISHING;
if (a_dns is dotted decimal)
return POSSIBLE_PHISHING;
if (a_link or v_link is encoded)
        { v_link2 = decode (v_link);
          a_link2 = decode (a_link);
          return LinkGuard (v_link2, a_link2); }
 /* analyze the domain name for possible phishing */
 if (v_dns is NULL)
return AnalyzeDNS (a_link);
 if (actual_dns in blacklist)
return PHISHING;
if (actual_dns in whitelist)
return NOTPHISHING;
return PatternMatching (actual_link);
```

3.3. Image Based Feature Extraction Algorithm

Image based features is imported to determine the real domain name of a visiting web pages. To extract image-based features efficiently, we assume that the image-based features must be seen in the very first page of web site. For example, we can always see the website logo, which is usually a common image features in the website of welcome page.

In our project we are going to compare the logo or text present on web page with the logo stored in database. If both are matched each other then it is safe for processing the banking functionality else it shows the message that this is a fake web page that you have visited and someone trying to steal your information after that it will redirect to the original web page.

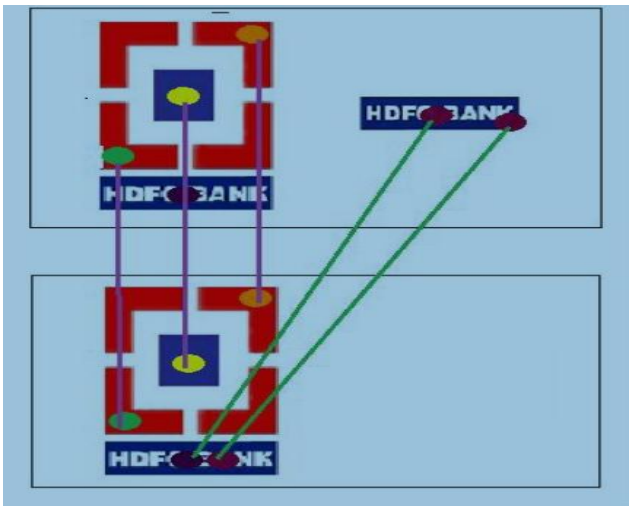

Fig.3: Image based feature Extraction. [2]

4. CONCLUSION

In this paper, we propose a solution that the Designed system improved the security power of original DES. The only drawback of Enhanced DES is extra computation is needed but the today's computer have parallel and high speed computation power so the drawback of the Enhanced DES algorithm is neglected because our main aim is to enhance the security of a system. By using the Enhanced DES algorithm the security is very tight and approximately impossible to crack and break the Enhanced DES algorithm. We have studied the characteristics of the hyperlinks that were embedded in phishing-mails. We then designed an ant 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. In Image Extraction a solution tries to reduce the number of password phishing attack by redirecting user to correct web pages. Site signature including text and image based features, are extracted accurately and use to identify the real domain name of the visiting web pages.

ACKNOWLEDGMENT

I would like to articulate our deep gratitude to my thesis guide Asst. Prof. Pradnya Mehta who has always been my motivation for carrying out the paperwork. I Special thanks to the institute, MMCOE, for giving me such a nice opportunity to work in the great environment. Thanks to my friend and colleague who have been a source of inspiration and motivation that helped me during my dissertation time. And to all other people who directly or indirectly supported and help me to fulfill my task.

REFERENCES

[1]. Manikandan. G, Rajendiran.P, Chakarapani.K, Krishnan's, Sundarganesh.G,"A Modified Crypto Scheme for Enhancing Data Security", Journal of Theoretical and Advanced Information Technology, Jan 2012.

[2]. Chun-Ying Huang, Shah-Pin Ma, Wei-Lin Yeh, Chia- Yi Lin1,Chien-Tsung Li, "Mitigate Web Phishing Using Site Signature". Department Of Computer Science And Engineering, Nation Taiwan Ocean University.

[3]. Sung-Jo Han, Heang-Soo Oh, Jongan Park," IEEE 4th International Symposium on Spread Spectrum Techniques and Application Proceedings ", 22-25 Sep 1996.

[4]. Alani, M.M.," A DES96 - improved DES security ", 7th International Multi-Conference on Systems, Signals and Devices, Amman , 27-30 June 2010.