ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

IARJSET

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Emerging Trends in Engineering and Technology (NCETET'16)

Lourdes Matha College of Science & Technology, Thiruvananthapuram

Vol. 3, Special Issue 3, August 2016

App for Monitoring Phishing Sites

Fahma Bakkar K A[1],Anjal thilakhan[2], Anjaly M S[3], Fasmina P M[4],Fathima Nasrin[5], Manu M R[6]

Student, Computer Science and Engineering, Royal College of Engineering and Technology, Thrissur, India[1, 2, 3, 4&5]

Asst. Professor, Computer Science and Engineering, Royal College of Engineering and Technology, Thrissur, India [6]

Abstract: Phishing is an online dishonest attempt that defrauds people of their personal information such as credit card number or bank account information. In olden days mass e-mailing with phishing link is the most popular way to lure the victims. Phishing is prevented by filter suspect emails in olden days. Fake browser tools have emerged new platforms among phishers. The Proposed System can control the running browsers on the PC using android mobile phone. It will restrict the access of phishing sites running in browser. The identification of phishing sites is through the comparison of Site URL with Blocked list and for security blocked URL list will be in encrypted form using DES Cryptography. While detecting phishing site on PC an alert message is sent to the mobile phones using gateway. By using android application admin will block the access on the phishing site. After blocking the site an acknowledgement will be send to the PC. If the site is not a phishing site it will redirect to the browser.

Keywords: Phishing attacks, URL, Encryption, DES algorithm.

I. INTRODUCTION

Today internet is unavoidable part of our life. Searching for information and also for entertainment internet is an unavoidable tool. Internet increases comfort of our life. When searching information always type a key word or any part of the URL. The related searches are listed down and click enter to get the site. In this searches no one will notice the slight changes in the URLs. It may be of phishing URLs.

Phishing is a tool to fool the users by creating clone of existing web pages and stolen their personal information. The user can't identify which one is the original site while seeing. But the URL of the original and clone is different. Sometimes any of the letter or the extensions are slightly modified by the phishers to fool the users.while comparing the original URL of Facebook with the phishing URL, identify an extra extension with the URL. But most of the people are not aware about the phishing sites, so they are not care this type of alterations in the site names. Blocking of the phishing sites have more importance than that of detecting a phishing site. Because on detecting a phishing site is not as much effective to get rid from phishing attacks.

App for monitoring phishing site is an effective way to detect and block the phishing sites. URLComparison is the method taken to detect the phishing sites. While entering the search key this typed URL is compared with the encrypted URL stored in the blocked list. if any matches is found then an sms is sent to the mobile phone including the detected site URL. Getting the alert the admin can log on to the app and block that site using the block button. If there is an option for allowing as in the case of any study purpose. Our experiment verified that this app is an effective method to prevent phishing attacks and ensures the protection of our PC.

Phishing can be done in many ways. Conventionally phishing is done by using by sending bulk e-mails. Nowadays replicas of sites are created by phishers. URL's are modified with unnoticed changes. The URLs are changed by adding an extra letter to the URL or by adding an extension after the URL. The paper concentrates on the phishing attacks which done by using altering the URL. Altering the URL will not be notified by any user in this busy world. While getting related URL, on clicking enter the user will get in to the site.

There are so many approaches to prevent phishers. One approach is to educate the users about phishing sites. This system can also punish the phishers legally, or by blocking the site on detection. Detect the phishing site running on PC and block the site using android app.
The remaining section is organized as: Section II proposed methods and the section III describes about the experimental results. Section IV explains related works. Finally, Section V concludes this paper.

II. RELATED WORKS

To get the knowledge about phishing concepts, techniques and anti-phishing techniques, literature survey is did on phishing by reading so many papers related with phishing. This section gives a brief description about some anti-phishing techniques.

Google Safe Browsing [6] uses a technique to detect phishing. Which is called blacklist anti phishing technique? The phishing URL is added in the blacklist for its presence. The URL is classified as legitimate URL if it is not found in blacklist otherwise classified as phishing website. Limitation of this approach is that phishing sites which are not added in blacklist are not detected. So the

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Emerging Trends in Engineering and Technology (NCETET'16)
Lourdes Matha College of Science & Technology, Thiruvananthapuram
Vol. 3, Special Issue 3, August 2016

system is not as much effective. Small change in the URL's with the black list will not be detected by the tool.
PhishShield[1] is desktop application for preventing phishing attacks. In this approach they mainly concentrate on URL and Website Content of phishing page. Here URL is taken as input and outputs the status of URL as phishing or legitimate website. The method used to detect phishing sites here are footer links with null value, zero links in body of html, copyright content, content in the title and website identity. PhishShield is an effective tool to detect zero hour phishing attacks which blacklists unable to detect. Visual based assessment techniques are slower than this method.

Another new method proposed is a end-host based anti-phishing algorithm, which is called as Link Guard[3]. They mainly concentrates on general characteristics of the hyperlinks in phishing attacks. The generic characteristics are derived by analyzing the phishing data provided by the Anti-Phishing Working Group (APWG).

Link Guard can detect not only known but also unknown phishing attacks. They have implemented Link Guard in Windows XP. Their experiments verified that Link Guard is effective method to detect and prevent whole known and unknown phishing attacks with minimal false negatives. This method experiments also showed that Link Guard is light weighted tool and can detect and prevent phishing attacks in real time.

Input of the the tool Phish Net[10] technique is black list. Phish net5 tool will predict the variations of each URL based on five URL variation heuristics such as Replacing Top Level Domain (TLD), similarity of directory structure, IP address equivalence, Query substituting string and Brand name equivalence. This technique can cover the limitation of exact match which is stated above in Google safe browsing. However, this technique has the same limitation of not detecting zero day phishing attacks.
PhishGaurd7 introduce a technique that large number of random generated credentials to the login form is feed, restricts user's original credentials from submitting and user want to wait for the response of server it chooses to feed the users credentials.

III. PROPOSED METHOD

A new app is introducing to monitor phishing attack to the PC of the user from anywhere. It provides security and minimizes number of phishing attacks delivered to users. There are mainly three modules.

- Home PC module.
- Online web Service Running Server Module.
- Android Mobile Module.

A. Home PC module
The main part of home PC module is creation of a web browser, for the purpose of setting access permissions. User registration is performed in Home pc module. On installing the web browser the user need to register with e-mail id and mobile number in which the app is installed. Only the registerd users can access the browser in the PC. At the time of registration he gets a password. This is the login password for the user. After login they can browse the sitesl. History of the search is stored as like every browsers. The URLs are stored in the blocked list in encrypted form using DES algorithm. Feistelcipher is included in Data encryption standard algorithm, with 64 bit block length and 56 bit key length. This algorithm takes 16 rounds to check with 48 bits of key used each round (sub key). A Feistel cipher is a general cipher design principle, not a specific cipher. Here the plaintext P is split into left and right halves,

$$P = (L0,R0) \quad (1)$$

, and for each round i = 1, 2, . . . , n are computed according to the rule for new left and right halves.

$$Li = Ri-1 \ (3.1) \quad (2)$$

$$Ri = Li-1 \oplus F(Ri-1,Ki) \quad (3)$$

where Ki is the subkey for round i. According to a key schedule algorithm the subkey is derived from the key K . The ciphertext C is the output of the final round,

$$C = (Ln,Rn) \quad (4)$$

Of course, it's nice to be able to decrypt.
And at the time of search if any URL matches with the encrypted one ie; any phishing site is detected the status is set to zero.
The zero statused URLs are sent as an alert to mobile phone using gateway. Phishing sites are already stored in the blocked in encrypted form. After blocking the site a blocked notification is received.

B. Online web Service Running Server Module.
In this module compare the current URL with already stored encrypted URLs. If the current URL is matched with the any one of the encrypted URL sending alert to mobile phone. The sms is sent via gateway. The sms contains the effected URL.

C. Android Mobile Module.
In android mobile module developing an app to block the phishing site. Using android studio developed an app to monitor the phishing site running on PC. The app also has a login password which the user got at the time of registration. when login to the app the admin can see the effected URL displayed in the screen. The displayed URL has the status of zero. On touch the admin is directed to the next page in which the URL is displayed with two buttons one for block and one for allow. If the admin click the block button the site will be blocked with changing the status to one. If any sites are urgent to visit then it is allowed the status changes to two.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
National Conference on Emerging Trends in Engineering and Technology (NCETET'16)
Lourdes Matha College of Science & Technology, Thiruvananthapuram
Vol. 3, Special Issue 3, August 2016

IV. EXPERIMENTAL RESULTS

A. Admin Login

Login in to the app is done by using the mobile number and otp generated at the time of registration.

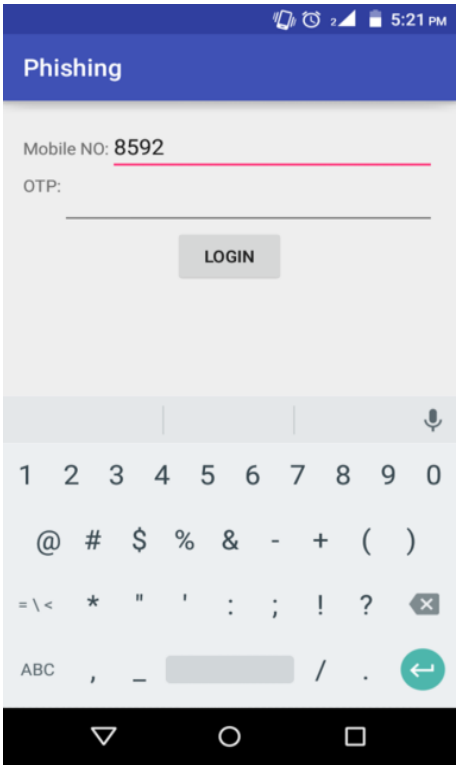

Fig 1.1This part is used for the registration purpose of user.

B. Detected site display

On login the admin is directed to this page. List of phishing sites detected are displayed in this page.

Fig 1.2 Detected phishing sites are displayed.

C. Allowing or block

On touch on the URL displayed in the second the admin directed to the page which shows the URL with a block and allow button. Clicking on the block button the site gets blocked in PC. In some cases admin can allow the site using the allow button.

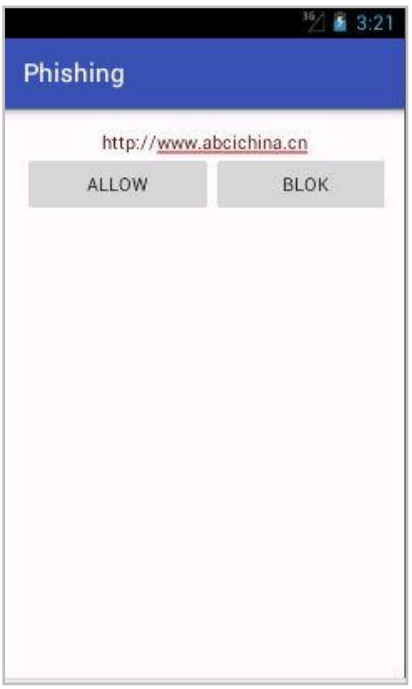

Fig 1.3 Detected phishing sites are blocked using block button

V. CONCLUSION

This paper shows successful implementation of detection and blocking methods used to prevent users from interacting with the phishing sites and protecting their PCs from phishers. Existing systems only detect the phishing sites running on PC. But this is not an effective method to protect our PC from phishing sites. In proposed system successfully block phishing sites at the time of access using mobile phone. Ensure privacy and protection to our system.

ACKNOWLEDGMENT

We express our sincere thanks to our guide and co-ordinators. A heartful and sincere gratitude to our beloved parents and friend for their tremendous motivation and moral support.

REFERENCES

[1] Routhu Srinivasa Rao* and Syed Taqi Ali PhishShield: A Desktop Application to Detect Phishing Webpages through Heuristic Approach, Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015).

[2] Jyoti Chhikara ,Ritu Dahiya ,Neha Garg Monika Rani.Phishing & Anti-Phishing Techniques: Case Study. International Journal of

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

National Conference on Emerging Trends in Engineering and Technology (NCETET'16)

Lourdes Matha College of Science & Technology, Thiruvananthapuram

Vol. 3, Special Issue 3, August 2016

Advanced Research in Computer Science and Software Engineering, 2013.

[3] U.Naresh1 U.Vidya Sagar2 C.V. Madhusudan Reddy3..Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm. IOSR Journal of Computer Engineering (IOSR-JCE) ,2013

[4] Kirda,Christopher Kruegel Technical University of Vienna. Protecting Users Against Phishing Attacks Engin. Oxford University Press on behalf of The British Computer Society 2005.

[5] Angelo P.E. Rosiello, Engin Kirda Christopher kruegel and Fabrizio Ferrandi."A Layout Similarity Based Approach For Detecting Phishing Pages". IEEE Conference on Security and Privacy in Communication Networks, Nice, France, September 2007.

[6] Safe Browsing API – Google Developer, [Online] Available at https://developers.google.com/safe-browsing/

[7] The Antiphishing Working Group (2004) Phishing Activity Trends Report, http://www.anti-phishing.org

[8] Dikean, N. (2005) The XULTU Tutorial, http://-www.xulplanet.com/

[9] Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh, and John Mitchell."Client-side defense against web-based identity theft".In 11th Annual Network and Distributed System Security Symposium(NDSS'04), San Diego, 2005.

[10] P. Prakash, M. Kumar, R. R. Kompella and M. Gupta, Phishnet: Predictive Blacklisting to Detect Phishing Attacks, In INFOCOM, 2010 Proceedings IEEE, pp. 1–5, March (2010).