A Survey on Phishing Attacks

Krutika Rani Sahu
Shree Vaishnav Institute of Science and Technology Indore (M.P)

Jigyasu Dubey
Shree Vaishnav Institute of Science and Technology Indore (M.P)

ABSTRACT

In the last few years a large number of internet users are increasing additionally different companies, banks and service providers are providing services online. So various sensitive and financial data are becomes online now in these days. This aspect of internet users are an evolution for us but the dark side of this advantage is too hard to accept, because of hackers and intruders are working between end clients and service providers. A secure and efficient technique is required to detect and prevent the attacks over the network transaction.

In this paper we make a survey about various attacks and their problems and establish a problem statement for finding the optimum solution for the problem arises. In addition of that here we propose a system architecture for future simulation of security in internet based security.

Keywords

Internet based security, phishing, detection, system architecture

1. INTRODUCTION

In today’s era everybody is using internet with the speed of generation like 2G, 3G, 4G, and many more and above. The Internet is a system of connected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billion users worldwide. Internet is in differential part of human life [2]. Because every age group person use it according to their interest or according to their requirement. Some of its applications like social networking sites by which anyone can connect chat or communicate over thousands of millions apart from each other. People use internet for saving their time and physical exertion by making online shopping, online banking, e-tickets and file transfer within friction of seconds by using e-mails etc. As internet shows such an advancements and facilities it also shows its dark side also. Some threats are also related to internet users [4].

As people use internet for their convince but there are some people whose intension is to harm other users for gaining money, to take revenge or some people do so just for fun using their skill in negative directions only. Person with bad intension known as hackers, crackers, intruders or malicious users, uses their technicality into negative directions [5].

Internet security is a branch of computer security. In this branch different types of cyber crime and miss uses of internet are tracked. As users of internet grow, frauds using internet also gain the advancement. In this study we present different types of frauds related to e-mails. As we all are using e-mails in our day to day life [6], for different purpose like official mails, personal mails or promotional or advertising mails. We got different mails in our inbox like advertising or promotional mails containing some offers to lure the user. This mails are not legitimate and number of peoples get trapped into such frauds because lack of knowledge about internet security. In this paper we discuss various attacks in internet based applications, their effect and detection and prevention techniques. In next section we discuss previously made efforts in the domain of providing security over internet based applications [8].

2. PHISHING ATTACK STAGES AND TYPES

There are different types of threats related to internet like malicious programs some of them using host program like trap doors, logic bombs and Trojan horses and some independent like virus, worms, and zombie. Phishing mails and spam mails are new type of attack on internet security or newly discovered threat for legitimate users. Before we discuss different types of phishing attacks we need to give definition of phishing attacks. There are different types of phishing definitions. As its name suggest we can define it like a trapped legitimate user who give away its personal detail over the duplicate web site. Which is very difficult to differentiate it from original one? First this attack is found at US where 57 million internet users have identified the receipt of e-mail linked to phishing scam and about 2 million of them are estimated to have been tricked into giving away sensitive information [5] [9]. As phishing crimes take place mostly with the help of spam e-mail messages.

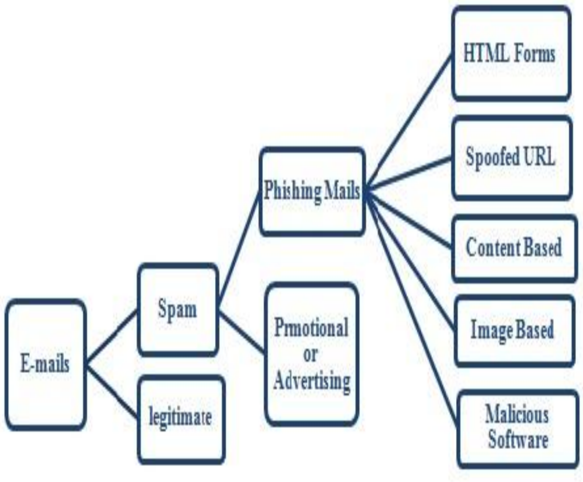

Fig 2: Classification of E-mails

But firstly we need to get clear on difference between spam mails and phishing mails. Spam mails or junk mails are used for advertising or promotional of some product or discount offers. The modified form of spam mails which harm the users financially known as phishing. So we can say that all spam mails are not phishing mails but all phishing mails are spam [10].

There are some popular methods of phishers to employ are as follows:

1) Impersonation: as we all know the meaning of impersonation that to be pretending someone else. This method is most easy and simple to execute. Now in case of phishing phishers construct web sites with the real images from original and might even linked to the real site.

2) Forwarding: is an e-mail we receive from Amazon, eBay and PayPal. Which is similar in images, graphics and login? When the victim logs in this forwarded links they directed to the fake server or to the person who is acting in between original sever and the victim this technique is known as man-in –the-middle.

3) Popup: this was essentially a link that you clicked within the e-mail which posts the hostile popup. The actual thought behind this popup to steal information. This is most authentic looking of the three approaches but now this is very in effective. Because most of the new browsers have popup blockers installed by default.

There are different stages to execute phishing crime successfully. First of all malicious user need to create a web site which is very similar in look and give very similar feel to the original website. Now the mailer mails some fraudulent offer to large number of users. Some legitimate users who aware of such crimes ignore these offers but some of them respond to such mails. By clicking on the given link in the web site they redirect to the false web pages in which they are asking for their credential information those are very personal to users like their banking account number, pin, and social security number etc. When the malicious user gets all such details it can miss use these details. As this type of fraud get discovered new techniques are found to protect legitimate users from these frauds but the malicious users moved a step ahead. Every time they came with new way to trick the legitimate users [3][6][8].

There is no thumb rule or a particular pattern which is followed by any phishers to employ successful phishing attack. There is a different type of attacks which is discussed into the following part of this study.

a. Man-in-the-Middle Phishing- as malicious user work in between the website and legitimate user. User is not able to make difference, and communicate to the fake person [5].

b. URL Obfuscation attack- as every spam mail contains an URL which is not original and user can’t find the difference. There are some methods of URL obfuscation:

   1. Bad Domain Names
   2. Friendly Login URL’s
   3. Third-party Shortened URL’s
   4. Host Name Obfuscation

c. Clint-side Vulnerabilities- there are number of functionality done on end user side as securities increased in browsers or we can say that number of built in security is provided in latest version of this browser.

d. Malware-based phishing- in this type of attack some malicious software get download on pc by just clicking on such mails. These type of vulnerability also harmfully to the system in which security application is not up to date [6].

e. Content-Injection Phishing- in this type of attack the malicious user change the some original content with fake content and misguide the legitimate users and make fool and phish them.

3. PHISHING DETECTION AND PREVENTION TECHNIQUES OR TOOLS

The first step is to detect the e-mails which give suspicious look and feel. Whether in mails. The phishing attack is very hard to detect in first attempt because it is very easy now a days to make the exact copy of original web site of banks, Amazon etc. now we need to go for their context if they ask for personal detail of users in the form of html form or offers some huge amount of jackpots and by checking the generic characteristics of the hyperlinks given in the e-mail. The systematic way to keep detection effective in different aspects is to watch or monitors account life cycle, Brand monitoring, Disables web duplication, Performs content filtering, Anti-Malware, Anti-Spam14].

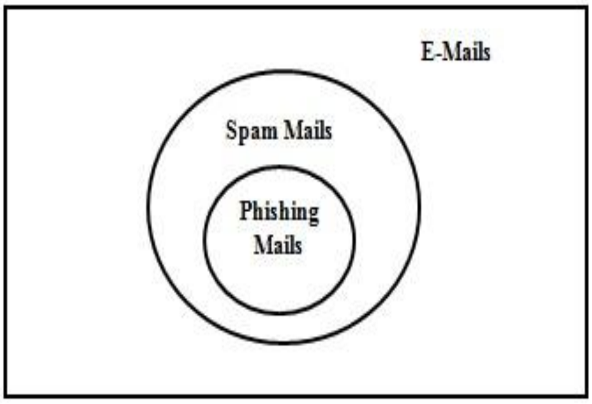

Fig 1: Relationship between Spam Mails & Phishing Mails

Since then the phishing attack is detected numbers of prevention methods are adopted but always a new type of fraud is evolved and all the old prevention gets failed. Some of the famous technical prevention solutions are adopted as follows:

i. Anti-Phishing Plug-in (Browser Extension): In this solution browser capability is extended. Now browses keep the track of users information and generates warning if found something is go wrong.

ii. Toolbars: In this solution toolbars are not able to classify contextual information which is done by e-mail filters. It simply generates truth rating related to the web-site which is dismissed by the user without paying attention to the warning.

iii. Phi stank: the place where all the information related to the links and name of spammer is placed who has done the phishing crimes in the past. The major disadvantage of this technique is that as information get older it gets deleted from the tank and if spammer use the same link after some interval of time then this link is new to the phi stank[6].

iv. Spam Filters: this solution is more effective than all the solution we have seen in our study by far because it works on the context of the e-mail and also observes the URL.

v. Machine Learning Algorithm: this solution work on prediction, based on known properties learned from the training data set.

As we discuss, all techniques involved in prevention of phishing attack. We adapt two social ways to reduce such scams. One by educating users and alert them about such threat. The second way is to punish phishing attackers legally [7].

Table 1: Details of Phishing Solutions

Phishing solutions	Functionality	Limitations
Anti phishing plug-in	Firstly discovered solution for phishing attack. Using as a browser extension or added functionality to the browser.	This solution only protects the inexperienced user from spoofed e-mails.
Anti phishing tool bars	Generate the passive warning against phishing attack.	This solution is not the active and can be easily ignored by the user.
Spam filters	These filters classify the mails before any harmful mail researches to the inbox. On the basis of previous data set filters can classify these mails.	This solution is firstly rule based and secondly based on machine learning mechanism. Both are not the perfect.
Prevention against Malware software	Some e-mails contains secrete code by clicking on such mails theses malicious software get automatically downloaded.	Use of some latest antivirus software to protect against such virus.

4. AVOIDANCE OF PHISHING ATTACK

Before being trapped into phishing attack we can work on its avoidance. After study lots of details about phishing we can avoid such conditions because of which user get into such crime. Different types are given as follows:

- Before responding: user gets very careful to respond on such e-mails who demand for personal information or offer some money.
- Typing of URL: never ever click on the URL given in the e-mails. Go to the URL by typing them into browser window. If there is any chance of difference in URL then it get reduced by typing it.
- Suspicious Website: if user find any suspicious about the web site then user can check for its authenticity. By checking its https in the beginning of URL, padlock icon in the browser any sign which makes it different from original site.
- Use of secure browser: user must use the browser with latest security against phishing attack Use latest versions of browser with updated phishing filter.
- Fantastic offer: don't believe such offers that are not easy to believe check for the all necessary details of the web site and ask too many questions before sharing any personal detail over the internet.

Avoidance is good option rather then gets trapped or become a fool.

In this study we can discuss and adopt some corrective solutions also. By taking site down and by investigating about such phishing sites.

5. CONCLUSION

In this proposed paper we discuss various issues and problems related to the phishing attacks and their roots are analyzed. To prevent the attackers and cyber attack we found out 10 of, 7 issues are related to the email spoofing, URL overwriting and email scams. Thus required provide a strong and efficient algorithm and data model which work on background of email service provider and analysis all the mails using hybrid architecture and classify the spam and dangers mails. But user must be careful when using internet and aware of such frauds.

6. FUTUR WORK

In the future we provide some technical solution by improve the efficiency of spam filters. By which too many mails are classified correctly and properly. By this legitimate user can surf internet with less fear.

7. REFERENCES

[1].Theodore S. Rappaport, Wireless Communications: Principals and Practice, 2nd ed., Pearson Education (Singapore) Pte. Ltd., India, 2002.

[2].C. Berrou, A. Glavieux and P. Thitimajshima, *Near Shannon limit error-correcting coding and decoding: turbo code*, Inter. Conf Commun., pp.1064-1070.1993.

[3]. D.C. MacKay, *Near Shannon limit performance of low density parity check Codes*, Electronics Letters, Vol. 32, pp. 1645-1646, Aug. 1966.

[4].C.E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J., Vol. 27, pp. 379-423 (Part one), pp. 623-656 (Part two), Oct.

[5].Upena Dalal, *Wireless Communication*, Oxford University Press, India, 2009.

[6]. Branka Vucetic and Jinhong Yuan, Space-Time Coding, John Wiley & Sons, 2003.

[7].Kai-Ting Shr, Hong-Du Chen, and Yuan-Hao Huang, *A Low-Complexity Viterbi Decoder For Space-Time Trellis Codes*, IEEE Transactions on Circuits and Systems-I, Vol. 57, No. 4, pp. 873-885, April 2010.

[8].N.Kumaratharan, S.Jayapriya and P.Dananjayan, *STTC based STBC Site Diversity Technique for MC-CDMA system*, IEEE Second International Conference on

Computing, Communication and networking Technologies, pp. 1-5, 2010.

[9].Pierre Viland, Gheorghe Zaharia and Jean-Francois Helard, *Improved Balanced 2n-PSK STTCs for Any Number of Transmit Antennas from a New and General Design Method*, IEEE Conference on Vehicular Technology, pp. 1-5, 2009.

[10]. Kabir Ashraf, *Different STTC over Rayleigh Fading Channels*, IEEE Conference, Dec. 2009.

[11].Pierre Viland, Gheorghe Zaharia and Jean-Francois Helard, *Coset Partitioning for the 4- PSK Space-Time Trellis Codes*, IEEE Conference on "Signals, Circuits and Systems, 2009.

[12].Thi Minh Hien Ngo, Gheorghe Zaharia, Stephane Bougeard and Jean Francois Helard *4-PSK Balanced STTC with two transmit antennas*, IEEE Conference, 2007.

[13].Murat Uysal, and Costas N. Georghiades, *On the Error Performance Analysis of Space-Time Trellis Codes*, IEEE Transactions on Wireless Communications, Vol. 3, No. 4, pp. 1118-1123, July 2004.

[14].J.N.Pillai and S.H.Mneney, *Adaptively Weighted Space-Time Trellis Codes*, Southern African Telecommunication Networks and Application Conference, Sep. 2004.

[15].Helmut Bolcskei and Arogyaswami J. Paulraj, *Performance of space-time codes in the presence of spatial fading Correlation*, IEEE Conference, Vol. 1, pp. 687-693, 2000.

[16].Murat Uysal and Costas N. Georghiades, *Error Performance Analysis of Space-Time Codes over Rayleigh Fading Channels*, Journal of Communications and Networks, Vol. 2, No. 4, pp. 351-356, Dec. 2000.

[17].M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels: A Unified Approach to Perform Analysis*, John Wiley & Sons, 2000.

[18].T. S. Rappaport, *Wireless Communications: Principles and Practice*, Prentice Hall, 1996.

[19].A. F. Naguib and R. Calderbank, *Space-time coding and signal processing for high data rate wireless communications*, IEEE Signal Processing Magazine, Vol. 17, No. 3, pp. 76-92, Mar. 2000.