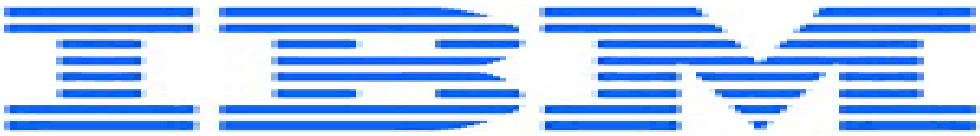

LITERATURE SURVEY

Team Members :
RAJALINGAM K
RITHIK KANISHKAR A
SYED AHMED KABEER
NAVEED AHMED

Web Phishing Detection

Literature survey

Rami M Mohammad, Fadi Thabtah, Lee MCCLUSKEY [1] : The Internet has become an essential component of our everyday social and financial activities. Internet is not important for individual users only but also for organizations, because organizations that offer online trading can achieve a competitive edge by serving worldwide clients. Internet facilitates reaching customers all over the globe without any market place restrictions and with effective use of e-commerce. As a result, the number of customers who rely on the Internet to perform procurements is increasing dramatically.

Aanchal Jain, Vineet Richariya [2] : Phishing is the combination of social engineering and technical exploits designed to convince a victim to provide personal information, usually for the monetary gain of the attacker. Phishing has become the most popular practice among the criminals of the Web. Phishing attacks are becoming more frequent and sophisticated. The impact of phishing is drastic and significant since it can involve the risk of identity theft and financial losses. Phishing scams have become a problem for online banking and e-commerce users. In this paper we propose a novel approach to detect phishing attacks. We implemented a prototype web browser which can be used as an agent and processes each arriving email for phishing attacks. Using email data collected over a period time we demonstrate data that our approach is able to detect more phishing attacks than existing schemes.

Gaurav Varshney, Manoj Misra, Pradeep K ATREY [3] : Phishing is a fraudulent technique that is used over the Internet to deceive users with the goal of extracting their personal information such as username, passwords, credit card, and bank account information. The key to phishing is deception. Phishing uses email spoofing as its initial medium for deceptive communication followed by spoofed websites to obtain the needed information from the victims. Phishing was discovered in 1996, and today, it is one of the most severe cybercrimes faced by the Internet users. Researchers are working on the prevention, detection, and education of phishing attacks, but to date, there is no complete and accurate solution for thwarting them. This paper studies, analyzes, and classifies the most significant and novel strategies proposed in the area of phished website detection, and outlines their advantages and drawbacks. Furthermore, a detailed analysis of the latest schemes proposed by researchers in various subcategories is provided. The paper identifies advantages, drawbacks, and research gaps in the area of phishing website detection that can be worked upon in future research and developments. The analysis given in this paper will help academia and industries to identify the best anti-phishing technique.

M Vijayalakshmi, S Mercy Shalinie, Ming Hour Yang, Raja Meenakshi U [4] : Internet dragged more than half of the world's population into the cyber world. Unfortunately, with the increase in internet transactions, cybercrimes also increase rapidly. With the anonymous structure of the internet, attackers attempt to deceive the end-users through different forms namely phishing, malware, SQL injection, man-inthe-middle, domain name system tunnelling, ransomware, web trojan, and so on. Amongst them, phishing is the most deceiving attack, which exploits the vulnerabilities in the end-users. Phishing is often done through emails and malicious websites to lure the user by posing themselves as a trusted entity. Security experts have been proposing many anti-phishing techniques. Till today there is no single solution that is capable of mitigating all the vulnerabilities. A systematic review of current trends in web phishing detection techniques is carried out and a taxonomy of automated web phishing detection is presented. The objective of this study is to acknowledge the status of current research in automated web phishing detection and evaluate their performance.

Aakanksha Tewari, AK Jain, BB GUPTA [5] : In the recent years, the phishing attack has become one of the most serious threats faced by Internet users, organizations, and service providers. In a phishing attack, the attacker tries to defraud Internet users and steal their personal information either by using spoofed emails or by using fake websites or both. Several approaches have been proposed in the literature for the detection and filtering of phishing attacks; however, the Internet community is still looking for a complete solution to secure the Internet from these attacks. This article discusses recent developments and protection mechanisms (i.e., detection and filtering) against a variety of phishing attacks (e.g., email phishing, website phishing, zero-day attacks). In addition, the strengths and weaknesses of these approaches is discussed. This article provides a better understanding of the phishing attack problem in the current solution space and also addresses the scope of future research to deal with such attacks efficiently.

Aanchal Jain, Vineet Richariya [6] : Phishing is the combination of social engineering and technical exploits designed to convince a victim to provide personal information, usually for the monetary gain of the attacker. Phishing has become the most popular practice among the criminals of the Web. Phishing attacks are becoming more frequent and sophisticated. The impact of phishing is drastic and significant since it can involve the risk of identity theft and financial losses. Phishing scams have become a problem for online banking and e-commerce users. In this paper we propose a novel approach to detect phishing attacks. We implemented a prototype web browser which can be used as an agent and processes each arriving email for phishing attacks. Using email data collected over a period time we demonstrate data that our approach is able to detect more phishing attacks than existing schemes.

R Suriya, K Saravanan, Arunkumar Thangavelu [7] : Phishing is a process of luring UNSUS in authentic looking email and messages for fraudulent purposes. Most preferred way that the phishers employ to lure victims is through a mass email, constructed to look like an authentic message from a well-known company. Phishing website has its own technical and social problem with each other and being a very complicate and complex issue to understand and analyze, to till date there exist no known single silver bullet to solve it entirely. Here an approach to create a resilient and effective method is proposed that uses fuzzy logic to quantify and qualify all the website phishing characteristics and factors in order to detect phishing websites to assess whether phishing activity is taking place or not. The approach visualizes the webpage in three layers of which the first layer, Domain Name checker, is fully based on characteristics of hyperlinks, the second, Code Script Checker which checks out for the tricks of the attackers in a way how they use JavaScript to hide information from user, and potentially launch sophisticated attacks, and the last layer of our approach, Page Content Checker, checks for phishing site based on its sub criteria. Finally if any of them (with regards to the true one) is higher than its corresponding preset threshold then that webpage reportedas a phishing suspect.

Reference :

1) Rami M Mohammad, Fadi Thabtah, Lee McCluskey,Computer Science Review 17, 1-24, 2015.

2) Aanchal Jain, Vineet Richariya, arXiv preprint arXiv:1110.0360, 2011.

3) Gaurav Varshney, Manoj Misra, Pradeep K Atrey, Security and Communication Networks 9 (18), 6266-6284, 2016.

4) M Vijayalakshmi, S Mercy Shalinie, Ming Hour Yang, Raja Meenakshi U , IET Networks 9 (5), 235-246, 2020 .

5) Aakanksha Tewari, AK Jain, BB Gupta Journal of Information Privacy and Security 12 (1), 3-13, 2016.

6) Aanchal Jain, Vineet Richariya , Implementing a Web Browser with Phishing Detection Techniques, ISSN: 2221-0741 Vol. 1, No. 7, 289-291, 2011.

7) R Suriya, K Saravanan, Arunkumar Thangavelu Proceedings of the 2nd International Conference on Security of Information and Networks, 193-1,2009.