Comparative Study of Phishing and Sybil Attack

Miss. Ankita S. Koleshwar Mrs. Swati S. Sherekar Mr. Vilas M. Thakare

Abstract **:- Nowadays, Internet is playing an increasingly significant role in on-line commerce and business activities. However, poor security on the Internet technology and the large financial gains provide a strong motivation for attackers. The frequency of Sybil and phishing attacks is noticeably increasing day by day. These attacks are becoming more destructor and unstoppable. It is very essential for companies to come up with new ways to solve these attack problems because it can become a major loss to well known companies. Not any type of technology can stop these types of attacks, but there are many ways to enable phishers from accomplishing their goals. Education it is very important for Internet users and e-mail users because they must have to aware about the activities involved in an attack. Consumer education can increase the awareness of the phishing threat and other online vulnerabilities. Phishing has resulted in lot websites frauds, now the condition is that people are going to do important transactions by using websites. For achieving the lost trust from naive users, capability must have improved to effectively fight out phishing and Sybil attack. The damage caused by phishing ranges from an internet user not able to access their email to losing all the money in their bank account. So according to all of these factors such as Financial sector, users account no information and all major concerns need heavy security.**

This paper focuses on structure, working, models, types, behavioral pattern, integrity, categorization and countermeasures of Sybil and phishing attacks.

Keywords **: Phishing attack, Sybil attack, Categorization, Anti-Sybil and Anti-Phishing techniques**

I. INTRODUCTION

Security is very important for today's network applications. The sensor and ad hoc networks are covered by the dangerous and harmful attacks like Sybil and Phishing attacks. Some types of security attacks attempt to disagree with accessing the appropriate user, either for the sake of inconveniencing them, or because there is some secondary effect [1]. Security indicates the need for protecting information from unauthorized access, use, exposure, interruption and variation. With this wide adoption of wireless networks in real-life applications, enforcing security in these environments has become a top priority.

There are various attacks which are very dangerous for the users who are on cloud. For the security point of view, attack prevention is very necessary. The attacks like Sybil, Phishing and lot more are affecting the performance of the systems. And now the security approach should be effective against this kind of attacks.

II. SYBIL ATTACK

Sybil attack is a type of attack in which an attacker manages to create and control more than one identity on a single physical device and it is a particularly harmful attack in sensor networks [2]. In a Sybil attack, an adversary creates a large number of fake identities saying here Sybil identities, and since all Sybil identities are controlled by the adversary, she can maliciously introduce a considerable number of false opinions into the system, and challenge it, by making decisions benefiting herself. Essentially, Sybil attacks break and manipulate the trust mechanism behind the systems.

III. PHISHING ATTACK

Phishing is a form of identity that uses the social engineering techniques and sophisticated attack vectors to collect financial information from innocent consumers. It is a kind of attack in which phishers use spoofed emails and fake web sites to trick people into giving up personal information. The phishing problem has evolved drastically over the past few years. This problem touches multiple points across the organization from end users and web sites to mail servers and networks [3]. In Phishing attack, criminals attract Internet users to websites that copy legal sites, are occurring with increasing frequency and are causing huge harm to victims. So the security must be needed on this type of attacks.

IV. CATEGORIZATION OF SYBIL ATTACK

The categorization of different types of Sybil attacks is discussed [4] and the capability of the attacker is determined by several characteristics which are as follows.

A. Insider Vs Outsider:

For an insider, the attacker holds at least one legal identity and claims that she receives certain data from the other nodes, by using the fake identities. Usually, a distributed system assumes that each node is trustworthy, and therefore, the false data can be forwarded to the entire system. However, for an outsider, she is an illegal entity; before launching a Sybil attack, she must first access the system.

B. Selfish Vs Malicious:

Selfish attackers control the false data just for their own benefit, while malicious attackers attempt to challenge a system. Whether an attacker is selfish or malicious is usually determined by the different types of targeted distributed system and final attacking effects.

C. Directed Vs Indirected Communication:

The attacker can directly communicate with an honest node by using one of her Sybil identities.

D. Simultaneously Vs Gradually obtained Sybil Identities:

The attacker can obtain all of her Sybil identities simultaneously, or she can gradually generate them one-by-one. For an intelligent attacker, the more diverse features the Sybil nodes have, the harder it is to identify Sybil nodes.

E. Busy Vs Idle:

All Sybil identities can participate in a distributed system simultaneously, or only some of them can work, while others are in an idle state.

F. Discarded Vs Retained:

For an attacker, the important issue is how to manage the old Sybil identity. After finding a Sybil node, one can gradually identify the others by monitoring the claimed communication between a suspect node and the detected Sybil node. Since the attacker is not aware of whether the old identities have been detected yet, once in a while, she has to determine whether or not to discard them.

V. CATEGORIZATION OF PHISHING ATTACKS

There are some types of phishing attacks [5] which are discussed below.

A. Keyloggers :

Keyloggers are spyware programs that install themselves either into a web browser or as a device driver. They are designed to record user input events and send them to a phishing server i.e., spyware owner. If a keyloggers gets into a corporate network, the data leaks could be catastrophic.

B. Rock Phishing Kit

In Rock phishing method, the phishing email points to a proxy that gets its content from a central spoofed website.

C. Torpig-Family Trojan

In this attack, the Trojan monitors major banks websites worldwide and after the users log in, displays a spoofed page while maintaining the original TLS session, thus being very difficult to detect. The Trojan spreads through operating system vulnerabilities.

D. Session Hijackers

In Session Hijacker attack users activities are monitored, typically by a malicious browser component. When the user logs into its account, or initiates a transaction, the malicious software "hijacks" the session to perform malicious actions once the user has legitimately established its credentials.

E. Content-Injection Phishing

In this attack, the malicious content can redirect to other sites, install malware on a user computer, or insert a frame of content that will redirect data to a phishing server.

F. "Universal" Man-in-the-Middle Phishing Kit

This kit consists of a PHP file which is installed on a compromised server.

G. Search Engine Phishing

In this phishing, phisher take an another approach i.e., to create web pages for fake products, get the pages indexed by search engines, and wait for users to enter their confidential information as a part of an order, sign-up or balance transfer.

H. Spear Phishing

In the spear phishing attack, it focuses on a single user or a department within an organization. Spear phishing scams will often appear to be from a well-known entity and may ask employees to update their username and passwords. Once hackers get this data they can gain entry into secured networks.

VI. STYLE & WORKING PRINCIPLE OF SYBIL & PHISHING ATTACK

A. Sybil Attack

The architecture & working principle of Sybil Attack is specified as follows:

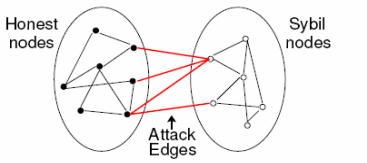

Figure 1: Architecture of Sybil Attack

As shown in the above figure, the social network with honest nodes and Sybil nodes are given [6]. Note that regardless of which nodes in the social network are Sybil nodes, which can always "pulling" these nodes to the right side to form the logical network in the figure.

B. Phishing Attack

Email is the main vector for delivering phishing messages to users. In a phishing attack scenario, attacker deceives users by a fake email which is called scam. [7] And for this scam detection, emails can be classified into three categories –

a) Spams
b) Scams
c) Hams

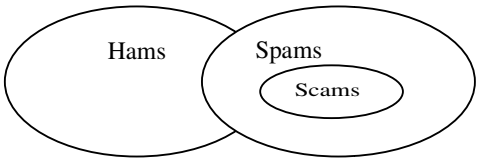

Fig.: email categorization

For considering the necessity of scam and spam detection, the data mining algorithms is to be used. They are Naïve Bayes, Poisson and K Nearest Neighbor [7].

VII. IMPACT ON SOCIAL NETWORK

Now, Mobile Cloud Computing offers the various services in very sensitive fields such as financial sector, banking, on line payments and all types of on-line transactions, which demands the critical security related vulnerabilities

within the mobile cloud computing platform. Nothing on the Internet is completely secured and even the biggest players suffer from serious attacks and security breaches [8]. The study is necessary on different types of attacks to improve the security.

Phishing is a form of online identity theft employing both social engineering and technical deception to steal user credentials such as usernames and passwords.

The damage caused by phishing ranges from an internet user not able to access their email to losing all the money in their bank account. So according to all of these factors such as Financial sector, users account no information and all major concerns needs heavy security. Anti-Sybil measures and Anti-phishing measures suggest protection against phishing and related aspects to avoid the phishing and provide safe environment for the internet users.

VIII. Detection Of Sybil Attack

The main difficulties in detecting Sybil attack come from various combinations of individual attacks. While it is difficult to link together multiple fake identities that appear in different periods of a networks. The identities established by a Sybil attacker — whether represented by IP addresses, MAC addresses, or public keys — differ from those of an honest node in several ways. Because the resources of a single node are used to simulate multiple identities, any particular assumed identity is resource constrained in computation, storage, or bandwidth.

In the mobile environment, a single entity impersonating multiple identities has an important constraint that can be detected: because all identities are part of the same physical device, they must move in unison, while independent nodes are free to move at will. As nodes move geographically, all the Sybil identities will appear or disappear simultaneously as the attacker moves in and out of range. Assuming an attacker uses a single-channel radio, multiple Sybil identities must transmit serially, whereas multiple independent nodes can transmit in parallel.

IX. Anti-Sybil Techniques

There are such Anti-Sybil techniques based on Social network are given as follows [9] :

A. SybilGuard & SybilLimit :

These are two famous Sybil defenses that use social networks. SybilGuard defines two terms – 1) a trusted path and 2) a trusted node.

B. SumUp :

SumUp is an Anti-Sybil technique designed for distributed voting system.

C. Canal :

Canal adopts a credit network, and we can regard it as an extension of SumUp.

X. Detection Of Phishing Attack

There are two detection mechanisms which represents the types of Anti-Phishing Applications [9]. They are as follows :

A. Blacklist-based anti-phishing application :

In this type of application, user gets warning when the URL of the visited page is in the list of already detected or reported phishing pages.

B. Whitelist-based anti-phishing application :

This type of application confirms the authenticity of trustworthy pages that have been saved in the whitelist.

Here now assuming that the blacklist-based anti-phishing is going to become helpful for users identify more phishing pages than the whitelist-based.

XI. Anti-Phishing Techniques

Anti-phishing provides several different techniques to fight against phishing. [10] The anti-phishing measures are discussed as follows:

A. Blocked Site lists :

Blocked site lists are popular response to the phishing problem. In such type of schemes, a single central database maintains a lists of fraudulent sites, browsers check this database before proceeding to a site.

Earthlink and Netcraft both provide these services, implemented on the client by a browser toolbar.

B. Site Information Indicator :

Site Information Indicator provide information about the site in the browser toolbar or status bar. The URL field is an indicator already present in all browsers; in theory, a user could check the domain name in the URL to avoid phishing attacks, but in practice, the URL bar provides little protection.

C. SpoofStick :

It is the extension of browser that displays the current site's domain name in large letters in the toolbar to make the identification task a little bit easier, but it still relies on the user's ability to distinguish legitimate and illegitimate domain names.

These are the three anti-phishing measures which are necessary to understand.

XII. Conclusion

The network offers the various services in very sensitive fields such as financial sector, banking, on line payments and all types of on-line transactions, which demands the critical security related vulnerabilities within the mobile cloud computing platform. Nothing on the Internet is completely secured and even the biggest players suffer from serious attacks and security breaches. The study is necessary on different types of attacks to improve the security on Mobile Cloud Computing. Specifically, how different attacks affect the performance of the network and find out the security measures which have not solved up till now. The technology is constantly

changing, and making a challenging task for researchers and hence we need this study to restrict the attacks and to improve the security.

Phishing is a form of online identity theft employing both social engineering and technical deception to steal user credentials such as usernames and passwords.

The damage caused by phishing ranges from an internet user not able to access their email to losing all the money in their bank account. So according to all of these factors such as Financial sector, users account no information and all major concerns needs heavy security.

The purpose of this paper is to discuss the Sybil attack and phishing attack with various issues like education, prevention, avoidance along with that e-mail categorization is very important based on that authenticity of the mail can be decided. Anti-Sybil measures & Anti-phishing measures suggest protection against Sybil & Phishing and related aspects to avoid the attacks and provide safe environment for the internet users.

REFERENCES

[1] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham Flaxman, "SybilGuard : Defending Against Sybil Attacks via Social Networks", SIGCOMM'06, ACM 1-59593-308-5/06/0009, pp. 267- 278, September 2006.

[2] Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam, Wade Trappe, "Channel-Based Detection of Sybil Attacks in Wireless Networks", IEEE Transactions on Information Forensics & Security, Vol. 4, No. 3, pp. 492-503, September 2009.

[3] Sujata Garera, Niels Provos, Monica Chew, "A Framework For Detection & Measurement of Phishing Attack", WORM'07, ACM 978-1-59593-886-2/07/0011, pp. 1-8, November 2007.

[4] James Newsome, Elaine Shi, Dawn Song, Adrain Perrig, "The Sybil Attack In Sensor Network : Analysis & Defenses", IPSN'04, ACM 1-58113-846-6/04/0004, April 2004.

[5] Pravin Soni, Shamal Firake, B. B. Meshram, "A Phishing Analysis of Web Based Systems", *ICCCS'1*, ACM 978-1-4503-0464-1/11/02, pp. 527-530, February 2011.

[6] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, Kashif Kifayat, "Lightweight Sybil Attack Detection in MANETs", IEEE Journal on Systems, Vol. 7, No. 2, pp. 236-248, June 2013.

[7] Hong Bo, Wang Wei, Wang Liming, Geng Guanggang, Xiao Yali, Li Xiaodong, Mao Wei, "A Hybrid System to Find&Fight Phishing Attacks Actively", IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, 978-0-7695-4513-4/11, pp. 506-509, 2011.

[8] Murat Demirbas, Youngwhan Song, "An RSSI-Based Scheme for Sybil Attack Detection in Wireless Sensor Networks", IEEE International Symposium on a World of Wireless, Mobile & Multimedia Network, 0-7695-2593-8/06, 2006.

[9] R. Suriya, K. Saravanan Arunkumar Thangavelu, "An Integrated Approach to Detect Phishing Mail Attacks – A Case Study", *SIN'09*, ACM 978-1-60558-412-6/09/10, pp. 193- 199, October 2009.

[10] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge, "Protecting People from Phishing : The Design and Evaluation of an Embedded Training Email System", ACM 978-1-59593-593-9/07/0004, pp. 905-914, April 2007.