International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 6 Issue: 3 175 - 178

A Review on Preventing Insider Threats and Stealthy Attacks from Sonet Site

Priyanka Sanjay Kasbekar
Computer Science and Engineering
P.R.Pote College of Engineering and Management, Amravati
Maharashtra, India
E-mail:pskasbe14@gmial.com

Rupali Shriram Saolikar
Computer Science and Engineering
P.R.Pote College of Engineering and Management, Amravati
Maharashtra, India
E-mail:rupalisaolikar01@gmail.com

Snehal Gajanan Kokate
Computer Science and Engineering
P.R.Pote College of Engineering and Management, Amravati
Maharashtra, India
E-mail:snehal2kokate96@gmail.com

Samiksha Baburao Boralkar
Computer Science and Engineering
P.R.Pote College of Engineering and Management,Amravati
Maharashtra,India
E-mail:samiboralkar@gmail.com

Prof. P. B. Sambhare
Computer Science and Engineering
P.R.Pote College of Engineering and Management,Amravati
Maharashtra,India
E-mail:sambharepraful832@gmail.com

***Abstract*—** Online social networks (OSNs) give another measurement to individuals' lives by bringing forth online social orders. OSNs have upset the human experience, however they have likewise made a stage for gatecrashers to disperse diseases and direct cybercrime. An OSN gives an entrepreneurial assault stage to cybercriminals through which they can spread contaminations at a huge scale. Assailants perform unapproved and malevolent exercises on OSN. Assaults can be an executable document, an expansion, an adventure code, and so on., that behaviors malignant tasks in OSNs with genuine effect on clients. Moreover, Intruders influence OSNs with different intensions, for example, to take basic information and adapt it for monetary profits. Insider dangers have turned into a genuine worry for some associations today. A model for OSN is to introduced to avoid insider danger misuses and to protect the classification. Multilevel security instrument is connected amid the enlistment and login level. At enlistment organize one time randomized alphanumeric watchword will be created and send to the clients by means of email though at login arrange randomized graphical secret word will be connected to counteract non malignant movement**.**

Keywords- *Social Networking,SONET,OSN, Attacks*

*****

I. INTRODUCTION

ONLINE social networks (OSNs) such as Facebook and Twitter provide a platform to attackers for spreading malware on a large scale. A particular attraction of OSNs is that users trust “friends” more than strangers, and the bad guys have figured out ways to exploit that trust. For example, increased trust increases the chance of a user clicking on a link that leads to malware. There are additional reasons why OSNs are attractive to attackers. First, OSNs have millions of users (Facebook with over 500 million and Twitter with over 106 million [3]) who regularly interact. Second, OSN users are highly interconnected; thus, information gets widely shared. Third, OSNs connect globally, with few restrictions among users across different geographical locations. Finally, information sharing is extremely fast. All these factors have attracted attackers to use OSNs as launch pads for broadly spreading malware across the Internet. In OSNs, users are the most valuable entity. OSNs are designed based on the concept of several sub networks (or islands) that are interconnected to form a single large network. OSN vendors have deployed some design constraints that need to be addressed before a user becomes a part of any specific network.

For example, permissions are required by users to become friends and build networks. Overall, it can be easily deduced that interconnected networks provide a large attack surface to attackers, which is why attackers treat OSNs as a lucrative platform to trigger attacks. The eventual goal of most OSN attacks is to exploit the trust of users and to perform nefarious activities such as:

1) The distribution of malicious messages with embedded links through tweets, rogue wall posts, online chats, videos, etc., that redirect users to malicious websites to infect end-user systems via drive-by download attacks [1]

2) Sending OSN-themed phishing emails for credential stealing and spreading malware through attachments;

3) Injecting unauthorized content in web pages for monetary benefits by increasing reputation through views and likes of posts and tweets;

4) Injecting malicious content (advertisements) from third-party websites [i.e., content delivery networks (CDNs)] to automatically include malicious content in a large number of user profiles;

5) Installing unauthorized applications in user profiles. A number of malware families that are used for targeting OSNs have been seen in recent years. For example, the Koobface botnet [4] spreads infections on Facebook by stealing users' credentials and then using them to log into accounts to spread spam with links to malware. Lily Jade [5] was designed as a cross-browser plug-in that used JQuery Web 2.0 application programming interfaces (APIs) and Cross rider plug-ins to send spam messages from active user accounts. Ramnit [6] targeted Facebook and stole thousands of user account credentials to exploit trust. These examples show that OSNs are already under different types of attacks. Insider threat [5] is a term coined from the threats that originate from inside an organization without the involvement of external actors. Insider threats are referred to employees or contractors with malicious intentions to disrupt organizations' operations and stature in the market. Insider threats emerge due to personal and organization factors. Insider threats can cause extensive damages to an organization. A recent research report published by SpectorSoft [5] revealed that organizations suffered approximately $40 billion in losses due to insider threats and frauds conducted by employees.

II. LITERATURE SURVEY

A. Background History

Insider threats can be motivated by several personal or organizational factors that cause employees to perform malicious activities such as stealing intellectual property, trade secrets, other employee's critical information, etc. Generally, anomalies generated in employee's behavior can be treated as indicators of strong suspicious activities. Social networks are used by many employees since from several decades, even on their organization's laptops and computer systems. In fact, the trend is even higher in technical companies compared to other employee's. It means that any existing threats on social networking websites are applicable to the employees residing in the organizations.

1) Insider threats share a malicious link on a social network website with the target present in the organization. Since the trust element is there as the link appears from the authorized profile, the target trusts the link.

2) The target clicks the embedded link, and the browser is redirected to the malicious domain.

3) Upon visiting the malicious domain, the malicious code inside the web page triggers a drive-by download attack and infects the target machine with socioware. The attack is executed in a stealthy manner, and the target is completely unaware of it.

4) Socioware becomes dormant and waits for the user to perform the desired actions. For example, socioware waits for the target to initiate some operations on the critical servers of the organization through proper authentication.

5) Socioware steals the login credentials and other sensitive information gathered from the infected target through system hooking and key logging to obtain the credentials of the target's account on the server.

6) Socioware also sends malicious messages from the infected target OSN profile to other users in the target's network. Since the trust element is inherently present, the infection becomes a chain infection.

7) Socioware transmits the stolen credentials in an encrypted format to the external server managed by the insider threat (or other supporting actors).

8) The insider threat obtains the target credentials that are used for accessing the internal servers of the organization that store highly sensitive information such as intellectual property, business documents, employees' details, etc.

9) The insider threat chooses the appropriate time and accesses the critical servers using the stolen credentials to download sensitive information.

10) The insider threat zips or encrypts the stolen data (or information) from the servers and transmits the data back to the external server. Since the insider threat is present physically, portable devices such as universal serial buses or storage cards can be also used to store the stolen data.

There are several reasons why this model results in successful attacks. First, insider threats have a lot of knowledge about the employees working in the organization, including their identities, working style, etc. Second, with the employees' information, it is not hard to trace or detect the employees' personal profiles on OSNs. Third, establishing trust with those employees on OSNs is not a hard task for the insider threat because all of them work in the same organization. Fourth, once the social network is formed with the organization employees, the trust is established, and information can be exchanged. Fifth, the majority of organizations allow their employees to surf OSNs from their internal network as this has become a de facto standard these days, except for few organizations that have very strict Internet surfing policies for security reasons. Sixth, socioware is not that hard to obtain these days. With the existence of the crime-ware as a service model [10], it is easy to place an order in the underground market to get some nefarious piece of malware by paying a small fee. Overall, any advanced insider threats can easily conduct these attacks to yield highly effective results.

A. Existing System

Trace-oriented simulation study: They conducted a trace-oriented simulation study using real-world data to understand malware propagation tactics, user click probability, change in social structures, etc., in OSNs. Malware Propagation: Their

study is more dedicated toward understanding the propagation of malware and the associated variations in the patterns of users on OSNs. They also discussed the performance issues related to various client-side and server-side defenses deployed to combat OSN malware. Network segmentation In addition, they also proposed a technique of network segmentation to sanitize the messages flowing between user's behavioral changes. They are more focused on the behavioral changes that happen in an OSN but did not provide any detailed classification of OSN malware and its inherent design. [1]

Bits: They introduced the notion of privacy "bits" for the characterization of various types of information shared among user profiles. They discussed the privacy leakages that happen in OSNs. Their work is focused on protecting the private information of OSN users. Third-party domains They also extended their work [4] by analyzing the various tactics opted by third-party domains via Hypertext Transfer Protocol (HTTP) header patterns such as request uniform resource identifiers, cookies, referrers, etc., to leak personal identifiable information. [2]

Log management technique: It introduced a log management technique to analyze the behaviors of insider threats that potentially exploit web servers for unauthorized operations. Web server logs: The approach required the analysis of web server logs and the correlation of events to detect an anomalous behavior. Log-based systems are effectively used as a part of security information and event management solutions. [3]

Frappe: In another research, they also introduced "FRAppE," i.e., Facebook's Rigorous Application Evaluator for detecting potential malicious Facebook applications. This research work did not discuss the root methods of how the Socware is created, generated, or distributed in the Facebook OSN. Infection: This study is mainly focused on the post infection scenario and how to detect potential issues but did not enlighten users on how the Socware reaches their profile and how the malware residing on end-user systems inject malicious posts by exploiting browsers, including various classes of OSN malware. [4]

Socware: He investigated Socware which pertains to nefarious, annoying, and most damaging posts posted by the friends of a potential victim. These posts can lead to malware, enticing users to provide information and false rewards, installing unauthorized apps, illegitimate task performance, and enhancing the reputation of posts by increasing the lies.

MyPageKeeper: They introduced a Facebook application known as "MyPageKeeper" that aims to fight against Socware and protects users on Facebook based on the concept of machine learning and data classification. [5]

A new technique suggested uses a combination of graph theory algorithms and machine learning in order to detect these types of users and does so by only using the graph topology structure. A unique technique having the combination of three different directed online social networks, each with a different level of anonymity. For each social network, our proposed method performed well when evaluated on both real and simulated profiles. A small number of profiles with a high probability of being fake or "spammer" profiles were extracted and analyzed. The analysis was performed by a team of experts with diverse backgrounds. According to the experts, evaluating a user's profile authenticity is a difficult task due to the fact that many fake profiles go to great lengths to appear legitimate. Only a thorough analysis of the few available details can reveal such a deception. For example, during the course of this research, they encountered a profile which appeared in several social networks, was very active, and had many friends. Only through the use of "photo watermarks" were we able ton uncover the fact that the picture actually belongs to a different user in a different country. In many ways, the identification of fake profiles can be described as a version of the Turing Test.[8]

In the Proposed system, applications are regarded as processes and Facebook social informatics as resources similar to an operating system. In that respect, FAITH functions as an application-level social-centric operating system kernel. FAITH augments the Facebook platform's management mechanisms of social data defending against privacy leaks and devaluation of social informatics. This paper has described how FAITH can be utilized to accomplish this. From the feedbacks we received, many users found FAITH useful in defending the privacy of their social data. We have also received many feedbacks about increasing the number of applications integrated with FAITH, which is certainly our goal. While we have received no complaints regarding performance during development, performance testing has demonstrated acceptable delays in processing time. [9]
Proposed system have evaluated how vulnerable OSNs are to a large- scale infiltrating by a Socialbot Network (SbN). We used Facebook as a representative OSN, and found that using bots that mimic real OSN users is effective in infiltrating Facebook on a large scale, especially when the users and the bots share mutual connections. Moreover, such social- bots make it difficult for OSN security defenses, such as the Facebook Immune System, to detect or stop anSbN as it operates. Unfortunately, this has resulted in alarming privacy breaches and serious implications on other socially-informed software systems. We believe that large-scale infiltrating in OSNs is only one of many future cyber threats, and defend-in

against such threats is the first step towards maintaining a safer social Web for millions of active web users.[10]

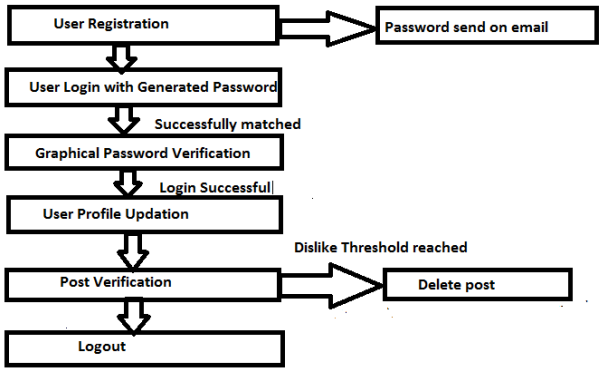
III. PROPOSED WORK

The basic focus of the suggested technique is to prevent activities which occur on SONET site, and to provide better security for login and registration phase. This project is going to develop a framework and a better software solution which will restrict all the unknown users to message directly. Along with this the post which consists of more number of dislike as compared to likes will be automatically detected and deleted.

3.1 Proposed System

It is based on the mechanism to enhance security mechanism for SONET sites. For achieving this level, this project will try to protect the user's confidentiality and privacy by applying multilevel security filters during the initial phase itself. once the profile is created again based on few parameters the post will be filtered and scrutinized.

STSYEM INFORMATION FLOW:



The proposed technique will work in the sequence given below .

1. User Registration & randomized onetime password(OTP) generation.
2. Cross verification of OTP password & graphical password selected at login phase.
3. User Profile Creation & Socialization.
4. Restricting Unknown Users to message the legitimate user until and unless they are friend of each other.
5. Identifying and deleting the post which is having more number of dislikes as compared to their likes.

IV. CONCLUSION

Here we are going to prevent various major threats which occurs OSNs. Understanding the OSN malware at this level of granularity helps researchers and security engineers design efficient security defenses because, with this taxonomy, the malware functionalities can be much better understood. Furthermore, we have discussed the design and nature of malware, direct, and indirect attacks to reveal how the security of OSNs is subverted by attackers. The design analysis detailed how the malware exploits OSNs' integrity by triggering infections in a number of ways. We have also presented a secured mechanism for safe login and registration activities of the legitimate user . Finally, we explored and proposed security solutions and countermeasures that are required to be implemented by OSNs to address the problems associated with malicious post by deleting it once the threshold for dislikes are reached so that secure environments can be provided to OSN users.

REFERENCES

[1] Aditya K. Sood, Sherali Zeadally and Rohit Bansal "Exploiting Trust: Stealthy Attacks ThroughSocioware and Insider Threats," IEEE Systems Journal,2015.

[2] Fredrik Erlandsson, Martin Boldt, Henric Johnson, "Privacy Threats Related to User Profiling in Online Social Networks," IEEE International Conference on Social Computing, 2012.

[3] Amirmohammad Sadeghian, Mazdak Zamani, Bharanidharan Shanmugam," Security Threats in Online Social Networks," IEEE,International Conference on Informatics and Creative Multimedia, 2013.

[4] J. Baltazar, J. Costoya, and R. Flores, The Real Face of Koobface Botnet,TrendMicro, Tokyo, Japan, White paper, 2009. [Online]. Available: http://goo.gl/IPRcRt.

[5] S. Golvanov, "Worm 2.0, or Lily Jade in action," Secure List Blog, May 2012. [Online]. Available: http://goo.gl/2ljT4N

[6] SpectraSoft, Insider Threat Survey, SpectraSoft Survey, 2012. [Online].Available: http://goo.gl/M40eCf.

[7] D. Cappelli, "Using empirical insider threat case data to design a mitigationstrategy," in Proc. ACM Workshop Insider Threats, Oct. 2010,pp. 1–2.

[8] Michael Fire, Gilad Katz, Yuval Elovici, Strangers Intrusion Detection – Detecting Spammersand Fake Profiles in Social Networks Based onTopology Anomalies.

[9] Ruaylong Lee, Roozbeh Nia, Jason Hsu, Karl N. Levitt, Jeff Rowe, S. Felix WuDesign and Implementation of FAITH, an Experimental Systemto Intercept and Manipulate Online Social Informatics.

[10] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, Matei RipeanuThe Socialbot Network:When Bots Socialize for Fame and Money.