A SYSTEMATIC REVIEW OF STUDIES ON PERCEIVED RISKS OVER ONLINE SOCIAL NETWORKS

Mr.J.S.Harilakshmanraj

Research Scholar,
Government College of Technology,
Coimbatore,Tamilnadu
India

Dr.S.Rathi

Assistant Professor(Sr.Gr)
Government College of Technology,
Coimbatore,Tamilnadu
India

Abstract

Online Social Network is one of the widely used information-sharing channels. Around, Billions of users share their contents, views and upload millions of multimedia contents to share with others every day. At present scenario, Cyber crimes like cyber-bullying and cyber-stalking activities are major threaten to society. In this paper, we present a thorough review of the different Cyber Crimes happens over OSN, which threaten OSN users in general as well as children in particular. In addition, we present an overview of existing systematic solutions that can provide better protection, safety, security measure and privacy for OSN users. Cyber Crime Security System (CSS) framework for OSN model is illustrated to improve their security and privacy over OSN environment. Furthermore, we suggest future research directions over OSN systems.

Keywords: Online Social Networks, Cyber Crime, CSS, Online Social Network Security Solutions.

I. INTRODUCTION

At present, Online social networks has increased widely these networks are interlinked with every people's life to share their thoughts, view and for other communication purpose. OSNs, such as Facebook[1],Google+ [2], LinkedIn [3], Twitter [4] and Tumblr [5] have billions of daily active users. Communication technologies have undoubtedly positively changed the way of users communication, it also provide *Intruders* with methods and techniques are been used for *unauthorized* purposes such as the distribution of offensive and threatening materials [12], spamming, phishing, cyberbullying, viruses, harassment and cyberstalking [14].

OSN users are unaware of the security risks,privacy risks [6], [7], identity theft [8], malware [9], fake profiles (also in some cases referred to as

Sybils [10], [11] or socialbots [6], [15], [9]), and sexual harassment [11], [15], among others.

Boshmaf *et al.* [6] and Elyashar *et al.* [13], [19], Facebook users have been shown to accept friendship requests from other users whom they do not know but with whom they simply have several friends or friends of friend (*fof*) in common. By accepting these friend requests, users unknowingly disclose their private information to strangers. This information could be used

wrongly, harming users in both in the virtual as well as in the real world. These risks intense more of users over OSN, especially young children or teenagers are been naturally more exposed and they have been threaten by vulnerable issues.

For example, organizational firm can use collected private information to combine with online ads according to a user's profile [18], to gain profit about their customers or even to share both user's personal as well as private data to government sector. [20]. This information may include general data, such as age, gender, and residential information. However, in some cases more delicate and highly harmful information can be relieved, such as the user's sexual orientation [21] and if the user have consumed addictive substances [22]. These privacy concerns become more wanted one, when considering the nature of OSN system and its framework. Information about network user can be obtained without even directly accessing the individual's online profile information such as personal details can be referred solely by collecting data on the user's friends [7].

To deal with the above-mentioned threats, number of solutions has been offered by OSN users, security companies, and academic researchers. Facebook, attempt to protect their users by adding Policy-based security authentication processes to ensure that registered user is a real person [6], [25]–[28]. Moreover, many OSN users also support configurable user privacy setting that enables users to protect their own personal data from other users within the network structure [29], [30]. As for privacy settings, OSN users currently face a problem of interest: One of the major issue is personal information is accountable, that is shared in open medium. On the other hand, user who is unease about his or her privacy is liability and will be probably share less amount of content and become consequently less pro-active. Nevertheless, both regulating authorities and public forums try to address privacy issues and make them a part of public concern and consideration [23].

II. MALWARE PRESENT IN OSN FRAMEWORK:

OSN threats can be categorized into four categories. The first category contains *Classical threats* namely, privacy and security threats willn't cause vulnerable to OSN users, it affects Internet users presented in social networks (see Section II-A). The second category covers *New-age threats* are isolated-one to the environment of OSNs and which use the OSN framework to more vulnerable user privacy and security (see Section II-B). The third category consists of *Tailored threats*, where we describe how today attackers combines various types of attacks in order to create more advance intruders techniques and *destructive attacks* (see Section II-C). The fourth category includes threats specifically Focusing over children who use social media (see Section II-D). Fig.1 illustrate outline of all categories of attacks and threats listed in the following Sections.

A. Classical Threats

This type of threats make of use of personal content posted by OSNs user and cause vulnerability towards user post and it leads to information disclosure. Spammers used to create fake profile pages to send illegal messages to OSN user. At, present spam rate have been increased rapidly [24]. Malware is malicious code deployed to interpret system process to gain access over user's private information.

B. New-age Threats

This threats cause vulnerability to OSN user as well as their own friend's private contents are also been disclosed. This type of attacking is known as chaining attack. Click jacking is a

endanger technique in which the event of clicking something, hijacks the users content from the source to the attackers. In such cases, if the information contains more authenticate (sensitive) data it will cause damage to the users account. De-Anonymization Attacks try to adapt users to the anonymity by De-anonymization strategy, such as tracking user cookies, network topology and memberships of the users group to disclose the user's real identity.

C. *Tailored Threats*

Attacker could combine two or more threats to perform destructive task over OSN environment. E.g. Phishing attack and click jacking, clone and spam, etc.,

D. *Threats over children's:*

Online Predators will create new group or forum, in that they will initiate to kidnap or murder teenage boys (or) girls, who have rich background. Cyberbullying is illegal task of posting or cause trouble over specific OSN user, by means of illegal tagging over image using their photo, posting unwanted content over user wall. These kinds of activities cause more harm to public network as well as it affect dignity of OSN's user.

III. **LAYERS IN CYBER SECURITY SYSTEM: (CSS)**

CSS is focused over safety of information and its controlling. Fig.2 illustrates overview of security layers and its functionalities. Information security solves the problems of information gathering, processing and sharing over non-destructive network environment. Its key point is to enhance existing privacy mechanisms, user privacy safety model, efficient manipulation of massive information encryption, etc. By controlling security over network solves the controlling problems in both systems which are open interconnected and loosely-coupled architecture. It focuses on overcoming the threats from attacks on system estimation and controlling algorithms.

Perception Layer:

In perception layer of CSS is closed system environment, it is composed with OSN network and interact with external users. It also depends on the *centralized node* of OSN network. Security issues of OSN network is unique factor to consider about design of security architecture and its layer framework. In CSS environment, perception layer is more threaten to external cyber-attacks. To establish intrusion detection and recovery mechanisms as well as to increase system robustness is another important issue in this layer. Establishing credibility model, to make behavioral assessment over suspicious nodes and deducing the impact of malicious behavior are important tasks in present in this layer.

A. *Network Layer:*

In network layer, OSN content and controlling commands are more sensitive. This Layer Consist of mechanisms like: mutual authentication between nodes, hop-to-hop encryption and cross-network certification. End-to-end security sub-layer could ensure the end-to-end privacy parameters to protect over network availability. Its corresponding security mechanisms include: end-to-end node encryption and key agreement as well as key management and cryptographic algorithm utilization. Finally, Detection and Prevention of Dos and DDoS attacks is achieved. Security mechanism for unicast broadcast and multicast are been designed according to the different network communication modes available over OSN environment.

Fig.1 Categories of Threats Presented in Online Social Media

B. Application Layer:

This layer follows certain Standard and principles of differentiated services. They offer different kind of security and privacy parameters. Even for same security services, there may be completely different context of different users. By providing targeted security services according to the user's need is core idea for the design of OSN framework. The main challenge over application layer include: hierarchical access over OSN content and privacy protection in the user authentication process are difficult in *OSN* network model.

IV. SECURITY RELAY SYSTEM FOR OSN ENVIRONMENT

This system consist of traditional data mining techniques like text mining, statistical analysis, text categorization and machine learning to overcome cyber issues especially cyberbullying and cyberstalking over OSN framework (Fig.3). It consists of five main modules: Detection module, Attacker identification, Personalization, Aggregator and messages. Final module is evidence collection, which consist of data-set and Meta-information about OSN user.

Fig.2 Layers in Cyber Security System

Unfortunately, due to character limitation of short messages like Twitter tweets, for e.g. SMS is limited upto 140 characters per message, writeprints doesn't provide enough information to identify the owner of the message.

A supervised algorithm is used for authorship identification. Identifying intruders is more difficult to detect malicious messages. Secondly, to identify and detect the user without prior knowledge is another difficult task. The system needs to decide whether a received message is written by intruder or not, thus supervised algorithms are not applicable. For this purpose, principal component analysis (PCA) is used to detect messages based on stylometrics and profiles. The new message's data is projected on PCA, and compared to the data matrix of all malicious messages in C_E .

Fig.3 Security Relay System for Controlling Cyber Attacks

V. RISK FACTORS AND ISSUES OVER OSN MODEL

A. Fake Customer Service Account

Fraudsters intercept the tweet with a link to a fake support site that tries to steal her actual bank account credentials.

Fig.4 Fake Customer Tweet**B. Posting fake comment**

Scammers often pretend to be facebook users, so they can comment on posts that lead to a credit card phish. So, phishing attack is also performed, while posting fake comments.

Fig.5.Fake comment over post**C. Financial phishing scams**

Fraudsters create fake social media accounts for real businesses like *Netflix* to carry out financial phishing scams.

Fig.6.Phishing scam in financial sites**D. Analysis over Spam Content**

Number of spam-target is much than spam followers; they overlap with the spam-targets. Consequently, *spam_rate* also increases in rapid manner.

Fig.7.Spam Target vs. Spam Followers

Numbers of spammers who rank within the top K ranks are plotted according to *pagerank* algorithm. In fig.8, there are seven spammers within 10,000 users, 304 spammers within 100,000 users and 2,131 users within 1million users.

Fig.8.Ranking spammers using Pagerank algorithm

VI. FUTURE RESEARCH DIRECTION IN SOCIAL NETWORK ANALYSIS

Social network analysis is current trending domain, it offer many paths to do research over tweet contents, comments posted over facebook timeline, examining vulnerabilities, malicious url,fake profile identification. Most cyber-crimes are performed over *OSN* affects user's profile and it leads to information disclosure. Cyber-crime activities such as *cyberbullying* and *cyberstalking* are major threaten to society. They are spread by spammers. Spam over *OSN*'s is discussed in (Section-V).

In *OSN* framework, progress tracking mechanism aren't been used for controlling cyber issues like cyber-bullying and cyber-stalking. So, there are many access control strategies, policy-ensuring mechanism, access control protocols are major techniques can used for ensuring protection over *OSN* framework. These technique can make *OSN* framework as secure and safety interface for communication.

VII. CONCLUSION

OSNs have become part of every human life and most of them spend more time on social networks than in any other online activity. Social networks have lot of cyber issues that have discussed in (Section-V). In this paper, we have presented scenarios which threaten *OSN* users and how users are cyber-bullied, posting malware messages over other user post, spreading of

spam over OSN are been described. Furthermore, we have provided examples of many of malware take place over OSN network. We have also explored some threats which challenge the safety of young children and teenagers across the OSN cyberspace.

VIII. REFERENCES

- [1]Facebook, accessed Jun. 14, 2016. [Online]. Available: <http://www.facebook.com/>
- [2]Google+, accessed Jun. 14, 2016. [Online]. Available: <https://plus.google.com/>
- [3]LinkedIn, accessed Jun. 14, 2016. [Online]. Available: <http://www.linkedin.com/>
- [4]Twitter, accessed Jun. 14, 2016. [Online]. Available: <http://www.twitter.com/>
- [5]Tumblr, accessed Jun. 14, 2016. [Online]. Available: <http://www.tumblr.com/>
- [6]Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, “The socialbot network: When bots socialize for fame and money,” in Proc. 27th Annu. Comput. Security Appl. Conf., 2011, pp. 93–102.
- [7]A. Mislove, B. Viswanath, K. Gummadi, and P. Druschel, “You are who you know: Inferring user profiles in online social networks,” in Proc. 3rd ACM Int. Conf. Web Search Data Mining, 2010, pp. 251–260.
- [8]L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, “All your contacts are belong to us: Automated identity theft attacks on social networks,” in Proc. 18th Int. Conf. World Wide Web, 2009, pp. 551–560.
- [9]J. Baltazar, J. Costoya, and R. Flores, “The real face of koobface: The largest web 2.0 botnet explained,” *Trend Micro Res.*, vol. 5, no. 9, pp. 200–219.
- [10]Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, “Aiding the detection of fake accounts in large scale social online services,” in Proc. 9th USENIX Conf. NSDI, 2012, p. 15. [Online]. Available: <http://dl.acm.org/citation.cfm?id=2228298.2228319>.
- [11]G. Stringhini et al., “Follow the green: Growth and dynamics in twitter followermarkets,” in Proc. Conf. Internet Meas. Conf., 2013, pp. 163–176.
- [12]O. D. Vel, A. Anderson, M. Corney, and G. Mohay. Mining E-mail Content for Author Identification Forensics. *ACM Sigmod Record*, 30(4):55–64, 2001.
- [13]A. Elyashar, M. Fire, D. Kagan, and Y. Elovici, “Organizational intrusion: Organization mining using socialbots,” in Proc. IEEE/ASE Int. Cyber Security Conf., 2012, pp. 7–12.
- [14]K. Reynolds, A. Kontostathis, and L. Edwards. Using Machine Learning to Detect Cyberbullying. In *Proceedings ICMLA 2011*, pages 241–244. IEEE, Dec. 2011.
- [15]Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu (2013, Feb.). Design and analysis of a social botnet. *Comput. Netw., Int. J. Comput. Telecommun. Netw.* [Online]. 57(2), pp. 556–578. Available: <http://dx.doi.org/10.1016/j.comnet.2012.06.006>
- [16]J. Wolak, D. Finkelhor, K. Mitchell, and M. Ybarra, “Online “predators” and their victims,” *Psychol. Violence*, vol. 1, pp. 13–35, 2010.

- [17]M. Ybarra and K. Mitchell, “How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs,” *Pediatrics*, vol. 121, no. 2, pp. e350–e357, Feb. 2008.
- [18]C. Tucker, “Social networks, personalized advertising, perceptions of privacy control,” presented at the 10th Workshop Economics Information Security (WEIS), Fairfax, VA, USA, 2011.
- [19]Elyashar, M. Fire, D. Kagan, and Y. Elovici, “Homing socialbots: Intrusion on a specific organization’s employee using socialbots,” in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining*, 2013, pp. 1358–1365.
- [20]C. C. Miller, *The New York Times*, Tech Companies Concede to Surveillance Program, Jun. 2013, accessed Jan. 14, 2014. [Online]. Available: <http://www.nytimes.com/2013/06/08/technology/tech-companiesbristling-concede-to-government-surveillance-efforts.html>
- [21]C. Jernigan and B. F. Mistree, “Gaydar: Facebook friendships expose sexual orientation,” *First Monday*, vol. 14, no. 10, Oct. 2009.
- [22]M. Kosinski, D. Stillwell, and T. Graepel, “Private traits and attributes are predictable from digital records of human behavior,” *Proc. Nat.Acad. Sci. USA*, vol. 110, no. 15, pp. 5802–5805, Apr. 2013.
- [23]J. Angwin and J. Singer-Vine, “Selling you on facebook,” *TheWall Street Journal*, Apr. 2012, accessed Jan.14, 2014. [Online]. Available: <http://online.wsj.com/news/articles/SB10001424052702303302504577327744009046230>
- [24]M. Fire, G. Katz, and Y. Elovici, “Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies,” *Human J.*, vol. 1, no. 1, pp. 26–39, 2012.
- [25]J. Constine, Facebook Launches Verified Accounts and Pseudonyms, Feb. 2012, accessed Jan. 14,2014. [Online]. Available: <http://techcrunch.com/2012/02/15/facebook-verified-accounts-alternate-names/>
- [26]A. Jeffries, “Facebook’s Security Check Asks Users to Identify Photos of Friends’ Dogs, Gummi Bears”. 2010, accessed Feb. 1, 2014.
- [27]J. O’Leary, Getting Started With Login Verification, May 2013, accessed Jan. 14, 2014. [Online]. Available: <https://blog.twitter.com/2013/getting-started-login-verification>.
- [28]A. Song, Introducing Login Approvals, May 2011, accessed Jan. 14, 2014. [Online]. Available: https://www.facebook.com/note.php?note_id=10150172618258920.
- [29]Y. Liu, K. Gummadi, B. Krishnamurthy, and A. Mislove, “Analyzing facebook privacy settings: User expectations vs. reality,” in *Proc. ACM SIGCOMM Conf. Internet Meas. Conf.*, 2011, pp. 61–70.
- [30]S. Mahmood and Y. Desmedt, “Poster: Preliminary analysis of google+’s privacy,” in *Proc. 18th ACM Conf. Comput. Commun. Security*, 2011,pp. 809–812.