A SURVEY ON VULNERABLE ATTACKS IN ONLINE SOCIAL NETWORKS

Dr.NaliniPriya.G[1] ,Asswini.M[2]

[1]Professor, Department of Information Technology,Saveetha Engineering college, Chennai,nalini.anbu@gmail.com

[2]PG Scholar, Department of software engineering, Saveetha Engineering College, Chennai,asswinimohan@gmail.com

***ABSTRACT*: An online social network(OSN) also referred to as a virtual community is a website on the Internet that serves as an ultimate location for people from different geometric locations to talk, share photos, ideas and interests, or make new friends. With the rapid increase in popularity and large number of user base, the online social networks also face an alarming rate of increase in security treats. The online social networking providers destine to secure their users; but the intruders and attackers are able to outsmart the security measures by exploiting user's privacy, identity and confidentiality using several techniques. Most of the users in social networking sites might be unaware of the existence of these critical threats. This paper highlights the major security issues concerning the online social networks. Also provides an overview of existing models that focus on ensuring security of user data.**

Keywords*: online social networks, privacy, security threats, user security, vulnerabilities in online social networking sites, authentication.*

I. Introduction:

An online social network (OSN)[1] can be defined as the use of dedicated websites and applications that allow the users to interact with other users, or to find people with similar interests to one's own. Since the evolution of web 2.0, the online social networking sites gained much popularity with the launch of the first social networking site in 1997[1], namely SixDegrees.com. The hierarchy of social networks inspires on achieving self-actualization, connect people from different places as well as ensure safety and esteem of the users.

The online social networks can basically be classified into two types namely: Traditional social networks[4](E.g. Facebook, MySpace, Twitter, Linked-in) and mobile social networks(MOSNs) such as watsapp,socialight[3],Dodge ball[3] etc. The main characteristics of these online social networks are: user-based, interactive, community-driven, relationship-based and emotion over content. There are a vast number of social networks available on the internet because of the phenomenal rise in the total count the of users. Based on the current research, the online social networks can be classified into 3 main categories namely: heterogeneous OSN[5],homogeneous OSN and social internetworking OSN[2].However the basic aim of these social networks is to protect the privacy of users and to provide security and interoperability thereby enhancing the reliability of the social networks.

The challenges vested on the internet are descending on social networks aswell.As the popularity of social networks is on air, people's interest in sharing of photos and personal information is also mounting. User creates personal profile and gets access into one of the available social networks and tries to explore users with homogeneous interest to introduce himself/herself [6]. The recent studies [8], [7], conclude that many OSN users endanger themselves by posting information such as family vacation, posting photos and personal phone numbers. Sometimes people accept friend request from unknown people [9] who may be the attackers, thus risking themselves [10].This enables the attackers to gain easy access to user's personal information with the help of social networks.

Though some attackers mine user's personal information for fun, the motive behind most of the attacks is harassment, steal personal information, company information [13], information related to bank accounts, security numbers and passwords. The third-party companies and social networking providers themselves may sometimes employ the use of user's personal information for the purpose of collecting information for marketing or for adds[11],also may also provide private information

978-1-4799-8788-7/15/$31.00/45 ©2015 IEEE

to the government when demanded[12].

Classification of Attack	Attack
classic treats	Internet fraud,spammer,malware, Phishing attack, cross-site scripting, SQL injection attack.
Recent trend attacks	Baiting, click-jacking ,doxing, elicitation, Pharming, phreaking, spoofing,identity-clone attacks, like-Jacking ,fake apps,Plug-in scam,identity-theft,socialbots, De-anonymization attacks.
Adolescent attacks	Cyber-bullying/stalking,online grooming,online-predators

Fig 1.Classification of online social networking attacks

In order to overcome the above problems the OSN providers try to provide the users with several security options in order to keep their personal information hidden from other users in the same social network.

The OSN providers also tend to protect their users from spammers [15] employing the use of social network analysis [16] and techniques used in spam filtering in email. The OSN providers also aim to protect the users from the most crucial attacks such as cross-site scripting attack [17] and SQL injection attack [18] that can be implanted into the master coding of the web page to hijack user account [19].

This paper will highlight the major security issues that affect the online social networking users. The Section 2 explores the security issues in detail. Section 3 portraits various models that were developed to ensure the security of users. The section 4 finally concludes the paper with an essence of observations.

II.Online Social Networks Security Threats

The OSN threats can broadly be categorised into 3 .They are classic threats, modern threats and adolescent threats.

A. Classic Threats

Classic threats are the ones that that have been around ever since the introduction of the internet. Classic threats contribute the installation of viruses with the help of external devices, or place malicious code in the user's browser or profile.

They include the XSS attacks/cross-site scripting attacks, internet fraud, spammer, malware attack, phishing attack and SQL injection attack. These are explored below.

Malware: A malware is a software specifically designed to steal a user's private information and damage a computer system aswell.Examples of these malware ranges from spyware that are planted to capture bank account details, credit card numbers etc.They also include several adware which when triggered leads to infected ad-ons.

Spammers: A spammer is someone who uses the electronic mailing services to spread unwanted messages and also advertisements. According to the recent research [20] most of the spammers rely on the OSN to create fake profiles and indulge in spamming activities.

Phishing attacks: Phishing is an attempt made by the attacker to obtain sensitive information such as passwords, username, credit card details, and sometimes money by masquerading as a reliable entity in an e-communication.

Cross-site scripting or XSS attack: In a cross-site scripting attack a malicious code is injected into a congenial websites [19][18].The cross-site scripting attack can be divided into two types namely stored XSS attacks and reflected XSS attacks. A Stored XSS Attack occurs when malicious code is stored on a server permanently. A Reflected XSS Attack is performed by the trick of making a person click on a malicious link; thereby the injected code captures the server then reflects the attack back to the target victim's browser.

SQL injection attack:SQL injection attack is the most basic attack whose ultimate target is the database and is carried out via input data from client to the browser or other applications. The damages by SQL injection attacks are increasing with the number of internet users [21].

Internet fraud: Internet fraud refers to the crime of usage of internet to carry out illegal activities. They are carried out with the intension of depriving a person's money and personal data. The U.S Justice department refers the internet fraud to any scheme that employs the use of one or more internet entities to put forth the fraudulent solicitation to victims,inorder to carryout fraudulent transactions.

B.Modern threats

The modern threats are the recently evolved and pervasive that are most sticky to the online social networks. There are several threats under this category. A few of them are explored below.

Clickjacking:Clickjacking used to steal user initiated clicks or the mouse clicks to carryout actions that the user may not be aware of or may be not interested in, was introduced by Robert Hansen and Jeremiah Grossman in the year 2008.clickjacking tricks the user by making them click onto attractive buttons and thus routing them into malicious sites[22].Many works have been carried on clickjacking so far. In[23] the author proposed solution for clickjacking with the scope of analysing millions of web pages that are unique.

Social-bots: A social bot is a kind of bot that is generated through a social network profile. A social botnet can be recognized as a group of social bots controlled by a single botmaster, which integrate them to execute malicious behavior,and simultaneously time mimicking the communication on ordinary OSN users in order to minimize the probability of being suspected and detected. In[23] the authors demonstrate the advantage and effectiveness of exploitation of social botnet for digital influence manipulation and spam distribution through real world experiments.

Fake profiles: Also referred to as the Sybil is the use of a person's personal information posted on the social networking profile to create a fake profile without the victim's knowledge[25].The fake profiles can be used to instantiate illegal ads, spread spam messages and friend request and may sometimes target the friend's of friends.The OSN providers aim to overcome these king of attacks by proper user authentication and validation.

Location and information leakage: The main advantage of the social networks allows the users to share a vast amount of information including personal information also proves to great insecurity for its users. The information shared via social networks can be mined by the attackers or the providers themselves for various purposes. For example the companies may use the social networking sites information for the purpose of selecting the applicant[27].information leakage may sometimes lead to inference attacks in which the attacks try to disclose the user's unrevealed information[26].The location based recommendation systems are becoming wide spread on the web with the advent of mobile social networks. The users unknowingly expose their location information when they share photos, multimedia, videos which are embedded with

"Geotagging" information and thus the user's current location can be easily computed [28].0

C.Adolescent attacks

As the popularity of the social networks is soaring high on cloud, the involvement of the adolescents in the social networking sites is increasing day by day. These social networks introduce the adolescents into new world of fatal perils such as cyber bullying and online grooming. Cyber bullying is when a personal, or a group of people, employ the use of internet, mobile phones or other digital technologies to induce fear, tease or abuse someone[29].The severity of cyberbullying attacks may sometimes lead to fatal consequences such as a person's death or suicide attempt. The cyberbullying attack can be classified into several types such as faming, denigration(spreading rumours),harassment, outing and trickery(disclosing private information),impersonation,cyberstalking(induce fear by sending offensive messages repeatedly over a period of time). Online grooming attack is when an adult approaches an adolescent online which the intention of seduction. In[30],the author uncovers three types of online predators or groomers based on the severity of risk asserted to the society. They are distorted attachment offender [30]:the person whom desires to establish a relationship with young people, adaptable online groomer[30]:who imagines the children as adults and try the hyper-sexualizes offender who posts pornographic contents. However with the lack in the image detection techniques, detecting the online groomers becomes a very difficult task.

III.Online Social Networks Security Techniques

Security concerns in the social networking sites are the main disadvantage behind them. Several authors have taken many steps to improve the security in the online social networks. Some of the approaches can be described as follows.

A. Watch dog and social enabler: These applications can be enclosed within the home network. It also acts an intermediately between the user and the OSN provider. It also helps the parents to prevent their children from adolescent threats.
B. User-control: These applications enable the users to control their settings. It enables the users to control what can be shared.
C. Structural anomaly detection: This approach enables the use of user behaviour monitoring in order to construct a probabilistic model. They employ the use of observations to detect abnormal events.
D. Virtual individual servers: The virtual individual servers enable the user to store the data in private individual servers restricts access of data to anonymous users.
E. Reputation mechanisms: The reputation mechanism is truly based on trust relationship. It is a main component of P2P communication.
F. Proxy-based protection: These provide real time protection to the user by blacklisting malicious sites.

IV.Conclusion

The online social networks have gained astounding popularity over the globe as the people tend to spend more time on the social networks. Thus the social networks have become inextricable part of everyone’s day to day life. With the raising futility there is also an alarming rate of increase in the insecurities with the use OSN.Once the users become aware of the possible attacks and the way of protecting themselves from the attacker, the online social networks would turnout be delightful experience for every user.

This paper presents the possible vulnerable attacks on social networks. These attacks have been classified under several categories thus making them easy to distinguish. Once the user understands the root cause of these attacks they can easily educate other users about these attacks.

V.References:

1.D.Boyd and N.B.Ellison,”Socil Networks Sites:Definition,History and Scholarship”,Computer-Mediated commun.,vol.no:13.2007.

2.Wu-Chen su.”Integrating and mining virtual communities across multiple online social networks:concepts,approaches and challenges”,IEEE,2014.

3. Laura Marcia Villalba Monné.”A Survey of Mobile Social Networking”.international journal of scientific engineering,2014.

4.yufeng Wang,Athanasios V.Vasilakos,Qun Jin,jianhuama,”Survey on mobile social networking in proximity(MSNP):approaches,challenges and architecture”,Springer,wireless networks,2014.

5.Han j,”Mining heterogeneous information networks:the next frontier”,proceedings of 18th ACM SIGKDD international conference on Knowledge discovery and data mining,ACM,China pp. 2-3,2012.

6. D. Boyd. Social Network Sites: Public, Private, or What? http://kt.flexiblelearning.net.au/tkt2007/edition-13/social-networksites-

public-private-or-what/.

7.A.Acquisti and R.Gross,"Imagined communities:Awareness,information sharing,privacy on the facebook",in Privacy Enhancing Technologies.
Springer-Verlag, pp. 36–58,2006.

8.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.*,IEEE pp. 93–102,2011.

9.A. Elyashar, M.Fire, D.Kagan, and Y. Elovici, "Organisation intrusion:Organisation mining using socialbots", in *Proc. IEEE/ASE Int. Cyber Security Conf.*, pp. 7–12,2012.

10.A. 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*, pp. 1358–1365,2013.

11.C.Tucker,"Social networks,personalized advertising,perceptions of privacy control", 10th Workshop Economics Information Security (WEIS), USA,2011.

12.C. C. Miller, The New York Times, *Tech Companies Concede to Surveillance Program*, Jun. 2013, accessed Jan. 3, 2015. [Online]. Available: http://www.nytimes.com/2013/06/08/technology/tech-companiesbristling-concede-to-government-surveillance-efforts.html.

13.Weimin Luo, Jingbo Liu, Jing Liu, Chengyu Fan," An Analysis of Security in Social Networks", IEEE 8th International Conference on Dependable, Autonomic and Secure Computing,2009.

14.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.*, pp. 61–70,2011.

15. A. Aggarwal, J. Almeida, and P. Kumaraguru, "Detection of spam tipping behaviour on foursquare," *22nd Int. Conf. World Wide Web Companion*, pp. 641–648,2013

16. K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: Social honeypots+ machine learning," *33rd Int. ACM SIGIR Conf. Res. Dev. Inf. Retrieval*, pp. 435–442,2010.

17. Tanmay S. Mule , Aakash S. Mahajan, Sangharatna Kamble, Omkar Khatavkar,"Intrusion Protection against SQL Ijection and cross-site scripting attacks using a reverse proxy", IJCSIT, Vol. 5 (3),2014.

18. Venkatramulu Sunkari & Dr. C. V. Guru Rao," Defensive Approaches on SQL Injection and Cross-Site Scripting Attacks", Global Journal of Computer Science and Technology: ENetwork, Web & Security,Volume 14,2014.

19. Martin, M., M. S. Lam, "Automatic Generation of XSS and SQL Injection Attacks with Goal-Directed Model Checking," 17th Conference on Security Symposium,2008.

20. 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.

21.Taiki Oosawa,Takeshi Matsuda,"SQL injection attack detection method using the approximation function of zeta distribution" ,IEEE International conference,2014.

22. Ubaid Ur Rehman, Waqas Ahmad Khan, Nazar Abbas Saqib, Muhammad Kaleem," On Detection and Prevention of Clickjacking Attack for OSNs",IEEE, 11th International Conference on Frontiers of Information Technology,2013.

23. Marco Balduzzi, Manuel Egele, Engin Kirda, Davide Balzarotti, Christopher Kruegel, (2010), A Solution for the Automated Detection of Clickjacking Attacks. [Online] Available at: <http:// www.iseclab.org/papers/asiaccs122-balduzzi.pdf> [Accessed January 5, 2014].

24. Jinxue Zhang, Rui Zhang, Yanchao Zhang, and Guanhua Yan," On the Impact of Social Botnets for Spam Distribution and Digital-influence Manipulation", IEEE Conference on Communications and Network Security (CNS),2013.

25. Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks", in Proceedings of the 18th WWW , pp. 551–560,2009.

26. 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*, pp. 251–260,2010.

27. J. Vicknair, D. Elkersh, K. Yancey, andM. C. Budden, "The use of social networking websites as a recruiting tool for employers," *Amer. J. Bus. Educ.*, vol. 3, no. 11, pp. 7–12, 2010.

28. G. Friedland and R. Sommer, "Cybercasing the joint: On the privacy implications of geo-tagging," in *Proc. 5th USENIX Conf. HotSec*, 2010, pp. 1–8. [Online]. Available: http://dl.acm.org/citation.cfm?id=1924931. 1924933.

29. Kamil Kopecký," Cyberbullying and Other Risks of Internet Communication Focused on University Students", Elsevier International conference,2013.

30. P. Gottschalk, "A dark side of computing and information sciences:Characteristics of online groomers," Journal of Emerging Trends in Computing and Information Sciences, vol. 2, no. 9, pp. 447–455, 2011.