International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT21732

A survey on : Online Social Networking Attacks Detection Techniques

Ankita Sharma
IEEE Member, Chandigarh University, Punjab, India

Article Info
Volume 7, Issue 3
Page Number: 44-50

Publication Issue :
May-June-2021

Article History
Accepted : 01 May 2021
Published : 05 May 2021

ABSTRACT

Today's due the popularity of internet number of users are increase on every social media platform. In recent research found that 80% of youth depend on social media to make new friends , share photos. Through this they get popularity and large number of user base and become influencers . Most of the social media platform are providing different privacy and security . Still attacker find out the way to breech the security, privacy and confidently of users and companies or organizations using several techniques . This paper highlight the major security issues phasing by many social networking web applications. Also identify the solution based on attacks in different literature . At last, we discuss open research issues

Keywords : Online social Networking, vulnerabilities , Attacks , Security Threats .

I. INTRODUCTION

Today peoples connected through virtual meeting environment with the help of global online social network (OSN) in recent years . These networks help many peoples to find their campaigns or friends globally and build a links worldwide. The important feature of the OSN is sharing the information and thoughts through Online platforms. Users can share there creative work , videos , interest , learning materials and much more which help the peoples worldwide. This was started in 1997 with sixdegree.com [1].That time connecting peoples from different countries is very inspiring to all .

The OSN is divided into two categories : web based Social network[2] (Facbook (2004)[3], twitter (2009), linkden(2006))and mobile based Social network[3] (whatsapp , social , telegrams)etc.Mostly users spend their maximum time on social networking sites . It helps in many way like exchanging the knowledge , education , searching the data without any barriers. But sometime many users start giving there so much information which may used by the attacker for malicious activity[4]. According to the one article[5] , the users accept the request without knowing that person.OSN. is targeting due to many reasons such as data breeching , information gathering . Due to the large amount of data available on social networking site such as name interest , age , gender , uploading personal photo of every places , educational information's and all sensitive information easily gather from OSN . The more data users broadcasting itself and come in the radar of attackers. These information make attacker to commit crimes easily.

Twitter[6] give the privacy to users that they does not allow to put personal details or information but issue is attacker can manipulate the posts and obtain what they want .Somya [10] discuss.

The challenge is to provide the privacy and security to the user in OSN and interoperability to enhancing the reliability of social network . The privacy become very important at every level of organization. According to threat report [10], 62.8 % peoples of organization use OSN to post huge amount of information due to this threat increase in OSN . In figure 1 we can see that the growth using OSN is increasing day by day by the report of statista [11].This report also discuss many other things such as number of active users in different Platform in Figure 2.

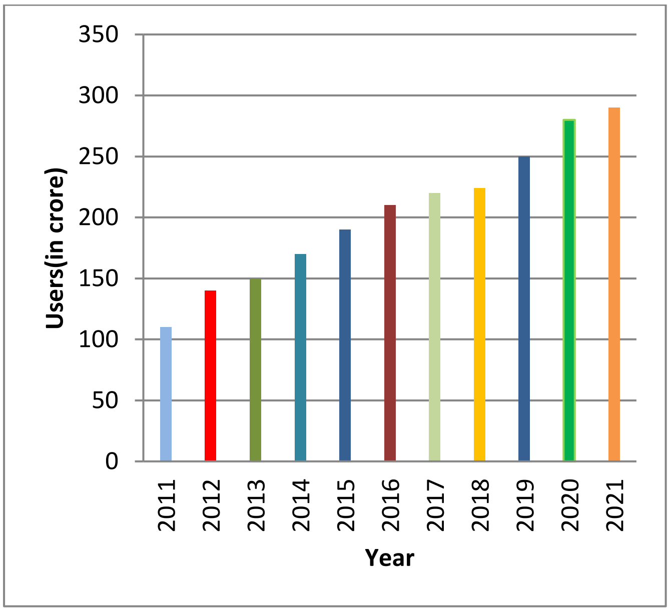

Fig:1 No of user Per year (In crore)

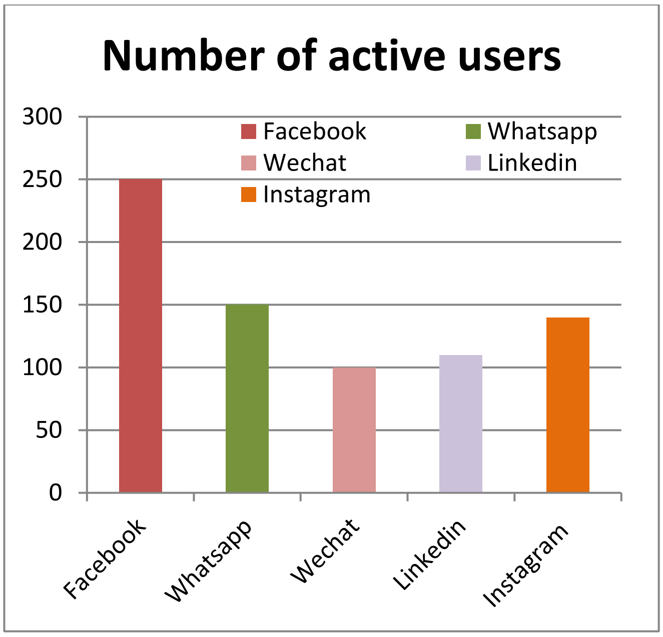

Fig 2 : Active Users in India in Different Platform

The remaining part of our paper is follow as: Section 2 discuss the various security issues and their solutions mention in different literature .After that we mention and future issues in section3. Section 4 finally conclude the research work with the essence of observation .

II. Online Social Network Security Threats

OSN is an interaction-based application that enable the register uses to interact with all ages of peoples in the network. It may be further divided into three category into 3 such as : classic threats , advanced persistent threat , modern threats .

Classic Threat : The structure of OSN , this threat grow very rapidly and circulate easily in the network among users. This threats affects users profile and credential by user personal information. It spread through clicking on malicious code or link . This threats is further classified into further category.

1. Man in the Middle Attack: This type of attack, is basically related to spamming and exploit OSN in large scale [12].

2. Phishing attacks: This type of attack is increase today at very fast rate such as more than 85% of organization suffered with this attack. The best way to

send the malware is through email attachments The attacker create the same social media website to get all the personal information [13].

3. Spamming Attack: The OSN users use someone electronic mail services to spread unwanted message and advertisement . According to many [14][15] many researcher found that attackers create a fake profile and indulge people in malicious activity without their knowledge .

4. Malware: It is a malicious code such as Trojan horses , virus and worms .This can spread through many users in internet[16].Most of the organization phasing this problem that they cannot protect the content flow from users to server.

5.Ransomeware: This kind of attack is also a malware but attackers block the access of computer until a sum of money is paid[17].

Advanced persistent : This type of threat attack the confidential information of users by pretending the genuine users in a wring manner [18]It is further divided into some attacks

1. Whaling attack: This attack gathering the users information from different OSN and pretend as a genuine users to get some confidential information.[19].This type of attack is collecting information of employee working some particular company.

2.DDoS attack: This attack is generating from many different locations which use users computer without their knowledge.

3.Speculation attack: It is geographical representation of users . When users increase , graph is also enhanced . Through this attackers find out the location of users and use.

4.Online chat Risk : This type of attack is sending unwanted malicious code in the chat box. These chat rooms are freely to send any content and users send there all personal details in these chat rooms.[20].

5.Vicinty Attack: Sharing information through OSN is main threat .The users need to secure their bank details , account number and all sensitive information .

6. Sybill attack : This attack is basically focus on peer to peer system and distributed environment[21]

Modern Threats:: These type of attack is basically related to OSN .

1. Clickjacking : This type of attack is done on mouse click . when users click on some unwanted adds and they may not aware about this type of attacks [22].

2.Social -Bots: A social botnets can be recognized as group , which execute the malicious behaviours and time mimickinmg [23].

3.Sql injection : This attack is target basically the backend by uploading some malicious data in the system [24].

4. Internet Fraud: The crime is useage the internet to carry out the illegal activities They are caried this with a bad intentions.

5. Cross- site scripting :In this attack malicious code is injected into a many website [25].

In the table 1. we are identify the attack with Mapping CIA and give solution in the literature. we Identify that which attack is very harmful in respect of CIA . and is any researcher work on the solution of these attacks.

Table 1 : Mapping Attacks with Solutions

Attacks	Layers			CIA			Solution	Features
	Classic	Advanced persistent	Modern Threats	Confidentially	Integrity	Authority (Authentication)		
DDoS		✓			✓		DDoS based detection	Network traffic
Spamming[14][15]	✓			✓		✓	Crowd based spammer [26]	Profile features, Content features

Phishing [13]	✓	✓				✓	Deepscan [27]	User accounts
Sybill[21]		✓			✓		P2P-based batch authentication [28]	Multiple authentication based data
Man-in-the-Middle [12]	✓				✓		-	
Click jacking [22]			✓	✓	-	✓	Automated detection [22]	Click on website by users
Cross site scripting [25]			✓	✓	✓	✓	Using reverse Proxy [31]	
Internet Fraud			✓	✓	✓	✓	-	
Vicnty		✓		✓		✓	Deep scan [27]	Location based data
Online chat risk [20]		✓					-	
Speculation [21]							-	
Sql injection[24]			✓		✓	✓	Approximation function detection anomaly [24]	Forms , Upload data
Social Bot[23]			✓			✓	Detection of human, legitimate bot and malicious bot in OSN based on Wavelet [29]	Discrete wavelength
Whalling		✓					-	
Malware	✓			✓		✓	DRIP[30]	Malicious accounts data
Ransomeware	✓			✓		✓	-	

In figure 3, we analyze that according to CIA how many attacker attack on which layer . So that researcher focus on that layer which have higher number of CIA chances .

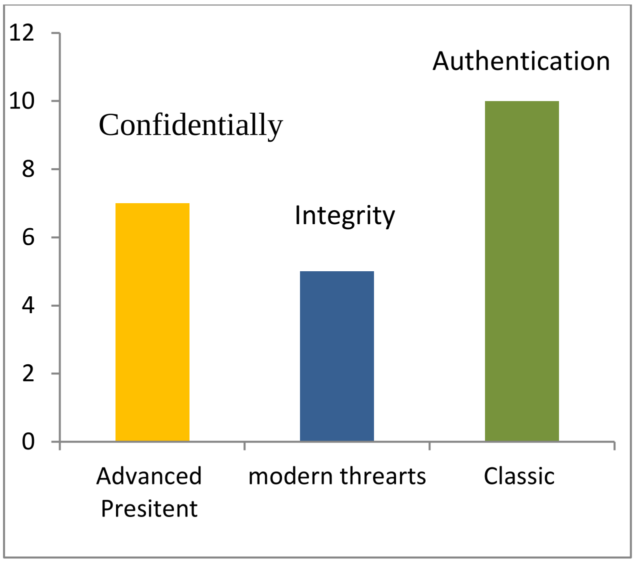

Fig 3 : Analyze of CIA with different Layer

III. Future work and Challenges

OSN is popular right now in researcher just because of popularity among many peoples for sharing and gathering information. Security researcher continuously working to secure the OSN from different threats .Since OSN have many issues which need to resolve such as:

1. Fake Profile : It is very difficult to identify that which account is genuine and which is legitimate account in the OSN especially Face book. So we need proper framework through which we can identify the accounts

2.Posting of Advertisement: It is very big challenge to identify that the post is nit containing any malicious code .Moreover many researcher working in this field .

3. Fake Website: Today Phishing is increase day by day and some time users get redirect to the malicious website that contain malicious code

So these are major area where researcher need to focus and find out the solution

IV. CONCLUSION

People spending there lot of time in surfing internet and use OSN to do their work in dailylife.OSN is becoming very addicted and some time helpful to users such communicate with each other when your love one is very far away .It help also in exchanging your knowledge without going anywhere in world. In this paper ,we presented the security attack phasing by Different OSN platform. We have outlined the different solution according to attacks. However at last we identify that what are the future work and challenges in this field .Overall , Researchers works in very suspicious way to find out the threats in OSN but still certain issues and resolved by using certain frameworks .

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]. Kefi, H., and C. Perez. 2018. "Dark Side of Online Social Networks: Technical, Managerial, and Behavioral Perspectives." Encyclopedia of Social Network Analysis and Mining 1–22.

[5]. Boshmaf, Y., I. Muslukhov, K. Beznosov, and M. Ripeanu. 2011, December. "The Socialbot Network: When Bots Socialize for Fame and Money." Proceedings of the 27th annual Computer Security Applications Conference, Orlando, FL (pp. 93–102). ACM

[6]. Twitter. https://twitter.com/

[7]. Facebook. 2018. "Facebook Security Products: Protect Your Computer with Free Security Software Downloads from Your Friends at Facebook." https://www.facebook.com/security/app_ 360406100715618

[8]. 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.

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

[10]. Sahoo, S. R., and B. B. Gupta. 2018. Security Issues and Challenges in Online Social Networks (Osns) Based on User Perspective. Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, 591–606. UNited Kingdom: CRC Press.

[11]. Statista report about online social networking users. https://www.statista.com/statistics/278414/ number-of-worldwide-social-network-users.

[12]. Beato, F., M. Conti, and B. Preneel. 2013. "Friend in the Middle (Fim): Tackling De-Anonymization in Social Networks." 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), San Diego, CA, March (pp. 279–284).

[13]. Tian, Y., J. Yuan, and S. Yu. 2016. "SBPA: Social Behavior Based Cross Social Network Phishing Attacks." 2016 IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, October (pp. 366–367)IEEE.

[14]. Fire, M., G. Katz, and Y. Elovici. 2012. "Strangers Intrusion Detection-Detecting Spammers and Fake Profiles in Social Networks Based on Topology Anomalies." Human Journal 1 (1): 26–39

[15]. 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

[16]. Baltazar, J., J. Costoya, and R. Flores. 2009. "The Real Face of Koobface: The Largest Web 2.0 Botnet Explained." Trend Micro Research 5 (9): 10.

[17]. Yang, T., Y. Yang, K. Qian, D. C. T. Lo, Y. Qian, and L. Tao. 2015. "Automated Detection and Analysis for Android Ransomware." 2015 IEEE 17th International Conference on High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conferen on Embedded Software and Systems (ICESS), Melbourne, August (pp. 1338–1343). IEEE.

[18]. Bilge, L., T. Strufe, D. Balzarotti, and E. Kirda. 2009. "All Your Contacts are Belong to Us: Automated Identity Theft Attacks on Social Networks." Proceedings of the 18th International Conference on World Wide Web, Madrid, April (pp. 551–560). ACM.

[19]. Williams, E. J., J. Hinds, and A. N. Joinson. 2018. "Exploring Susceptibility to Phishing in the Workplace." International Journal of Human-Computer Studies 120: 1–13. doi:10.1016/j. ijhcs.2018.06.004

[20]. Humphreys, L. 2007. "Mobile Social Networks and Social Practice: A Case Study of Dodgeball." Journal of Computer-Mediated Communication 13 (1): 341–360. doi:10.1111/j.1083-6101.2007.00399.x

[21]. Alghamdi, B., J. Watson, and Y. Xu. 2016. "Toward Detecting Malicious Links in Online Social Networks through User Behavior." 2016 IEEE/WIC/ACM International Conference on

Web Intelligence Workshops (WIW), Omaha, NE, October (pp. 5–8). IEEE

[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]. inxue 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.

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

[25]. Martin, M., M. S. Lam, "Automatic Generation of XSS and SQL Injection Attacks with GoalDirected Model Checking," 17th Conference on Security Symposium,2008.

[26]. Liu, B., Z. Ni, J. Luo, J. Cao, X. Ni, B. Liu, and X. Fu. 2018. "Analysis of and Defense against Crowd-Retweeting Based Spam in Social Networks."

[27]. Gong, Q., Y. Chen, X. He, Z. Zhuang, T. Wang, H. Huang, . . . X. Fu. 2018. "DeepScan: Exploiting Deep Learning for Malicious Account Detection in Location-Based Social Networks." IEEE Communications Magazine, Feature Topic on Mobile Big Data for Urban Analytics 56 (11): 21–27

[28]. Yeh, L. Y., Y. L. Huang, A. D. Joseph, S. W. Shieh, and W. J. Tsaur. 2012. "A Batch-Authenticated and Key Agreement Framework for P2p-Based Online Social Networks." IEEE Transactions on Vehicular Technology 61 (4): 1907–1924.

[29]. Liang, H., Z. Chen, and J. Wu. 2018. "Dynamic Reputation Information Propagation Based Malicious Account Detection in OSNs." Wireless Networks 1–14

[30]. Campos, G. F., G. M. Tavares, R. A. Igawa, and R. C. Guido. 2018. "Detection of Human, Legitimate Bot, and Malicious Bot in Online Social Networks Based on Wavelets." ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 14 (1s): 26.

[31]. 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.

Cite this article as :

Sh
Ankita Sharma, "A survey on : Online Social Networking Attacks Detection Techniques", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7, Issue 3, pp.44-50, May-June-2021. Available at doi : https://doi.org/10.32628/CSEIT21732
Journal URL : https://ijsrcseit.com/CSEIT21732