iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** V **Month of publication:** May 2021

DOI: https://doi.org/10.22214/ijraset.2021.34537

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

Big Data Mining of Social Networks for Threat Perception and Analysis

Miss. Pragati D. Bharsakle[1], Dr. M. A. Pund[2]
[1, 2]*Computer Science & Engineering, Prof. Ram Meghe Institute of Technology & Research Badnera, Amravati*

Abstract: Many users of social Network are not aware about the number of security risks in networks such as identity theft, privacy violations, sexual harassment etc. Recent studies says that most of the social network users expose their personal information like their date of birth, email address, phone number, relationship status. If this type of data reached to the wrong person, then person used that information to harm the users. If the children are users of social network, then these risks become serious. In this paper we present an approach and interpretation of threats.
Keywords: Social Networks, Security and Privacy, Security Threats.

I. INTRODUCTION

Social networks such as Twitter [5], LinkedIn [3], Facebook [1], Google+ [2], Sina Weibo [4], Tumblr [6], and VKontakte (VK) [7] have daily millions of active users. Facebook for example, has monthly active Facebook users numbered 2.45 billion as of oct. 2020. 350 million photos per day have been uploaded to the facebook by users. Unfortunately many users are not aware about the security risks that live in these kind of communication involving identity theft [14], malware [15], privacy risks [12], [13], and sexual harassment [20], [21], among others. A study of Dwyer et al. [22] detected that Facebook and MySpace [23] users belief these social networks and they have faith on other users within these networks. This fait leads to developing the new relationships and to sharing the information. According to studies [12], [24], many users reveal their personal information, their relationships, friends whether by providing information such as phone number, address, date of birth or by posting photos. Moreover according to Boshmaf et al. [12] and Elyashar et al. [19], [25], users of Facebook have been discover to accept friend request from people whom they do not know but with whom they have common friends. By accepting the requests, users unknowingly expose their private information to strangers. This information could be harming the users both in the virtual and in the real world. These risks shoot up when the users are young children or teenagers.

As the social networking use becomes increasingly more immersed in users' daily lives, personal details becomes disclose and mishandle. Information gather by both network operator and by third party, has recently been recognize as a notable security concern for social network users. Third party companies can use the gathered information for various intentions, all of which can threaten a network user's privacy. Consider the example, companies can use gathered data to customize online ads according to the profile of user [26] to achieve beneficial comprehension about their customers, or even to share user's private data [27]. This data include general information like gender, income, age; however in some cases more elegant and harmful data can be disclosed [28].

II. SOCIAL-NETWORK MANIPULATION

Social networks have millions of registered users. For example, Facebook is the largest social network in the world and has more than billion active users [30]. A survey by the Pew Research Center's[31] disclose that 72% of adults in America use social networking sites while in 2005, only 8% adults use social networking sites. Moreover survey disclose that the 89% adults between the age 18 to 29 use social networking site while in 2005 9% adults use social networking sites.

Mobile devices are the platform for internet usage. According to report [8] in December 2013, an active mobile user of Facebook was 556 million per day. Use of online social network on mobile devices such as smart phones promotes closer relationship to social network as well as it can pose additional privacy concerns, especially identity of user.

III. THREATS

Today, with the increasing use of social network, many users have exposed to threats to their privacy as well as their security. Threats can be categorize into four types. First type consists of classic threats which are privacy and security threats. Second types are modern threats who are unique to social network environment. Third type consists of combination threats, where we describe how attackers combine various types of attacks to create more sophisticated attacks. The fourth types of threats are targeting children.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue V May 2021- Available at www.ijraset.com

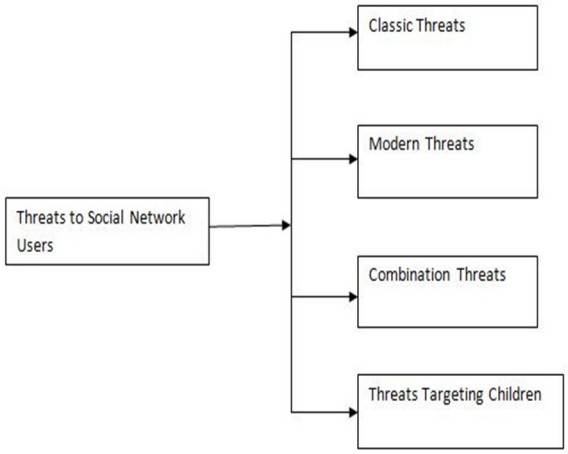


Figure1: Threats to Social Network Users

A. Classic Threats

With the widespread usage of internet classic threats have been a problem. Classic threats are malware, spam, cross-site scripting attacks, or phishing. These threats continue to be an ongoing issue. Due to the nature and structure of social network, these threats become increasingly viral. Classic threats take an advantage of personal details of user that are uploaded on social network to attack on both the user as well as user's friends by adjusting the threats.

For example, inside a spam message an attacker can fix a malicious code that appoints user's details from his or her facebook profile. Because of nature of message there are the chances that innocent user will open the message and get infected. These types of threats can use the user's stolen information to post messages on the behalf of user.

Different classic threats are described below:

1) *Malware:* Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for "malicious software." Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. In some cases, the malware can use the obtained credentials to impersonate the user and send contagious messages to the user's online friends. Koobface was the first malware to successfully propagate through OSNs such as Facebook, MySpace, and Twitter. Upon infection, Koobface attempts to collect login information and join the infected computer in order to be part of a botnet [15], a so-called "zombie army" of computers which often is then used for criminal activities, such as sending spam messages and attacking other computers and servers over the Internet.
2) *Phishing Attack:* Every day, email inboxes fill up with annoying, unwanted messages. However, some of these junk messages are malicious/ phishing attacks. By using phishing emails, texts, or social media posts that lead to phishing sites, fraudsters attempt to deceive user into revealing his/her personal and sensitive information – bank account numbers, credit card info, Social Security number, or login IDs, usernames, and passwords. Once obtained, they use credentials to steal user's money, his/her identity, or both.
3) *Spammers:* Anyone who uses email encounters spam, also known as junk mail. At the very least, it fills in boxes and takes up valuable time; at its worst, it tricks unsuspecting recipients into divulging private information or sending money to an unknown party. Spam is so pervasive that most email providers supply spam-reporting and blocking tools.
4) *Cross-Site Scripting (XSS):* Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.
5) *Internet Fraud: Internet Fraud:* Is a type of cybercrime fraud or deception which makes use of the Internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance.

B. Modern Threats

To the social networks a typical unique threats are modern threats. These threats target not only the personal information of user but personal information of their friends also. For example, an attacker can try to access user's personal information which is viewable only to the user's friends. To access user's information attacker can create a fake profile and initiate a friend request to targeted user. If user accepts the friend request his or her details will be shown to the attacker. Alternatively user can collects data from user's friend.

Various modern threats are illustrated as follows:

1) *Clickjacking:* Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.
2) *De-Anonymization Attacks:* particular form of inference attack called the de-anonymization attack, by which an adversary tries to infer the identity of a particular individual behind a set of mobility traces. For ex. Sharing sequencing data short tandem repeats on the Y chromosome and querying recreational genetic genealogy databases. It is shown that a combination of a surname with other types of metadata, such as age and state, can be used to identity of the person...
3) *Face Recognition:* Many people upload their pictures on social networking sites. And their pictures are publically available to view and download. An attacker can use these photos to create biometric databases which can then be used to identify social network user without their consent.
4) *Fake Profiles:* Fake profiles are used to gather users' personal information from social networks. By sending a friend request to other users, who often accepts the requests, an attacker can collect a users' personal information that should be exposed to only users' friends. Furthermore, fake profiles can be used to create Sybil attacks.

C. Combination Threats

To create more sophisticated attacks, hackers can combine classic and modern threats. For example, to collect Facebook password of user, an attacker can use phishing attack. And to post the message on user's timeline, he or she uses clickjacking attack. Thus luring the user's friends install hidden virus onto their computers by click on the post.

D. Threats Targeting Children

Children, either young or teenagers, experience the classic and modern threats, but there are also some threats that intentionally target the young users of social networks.

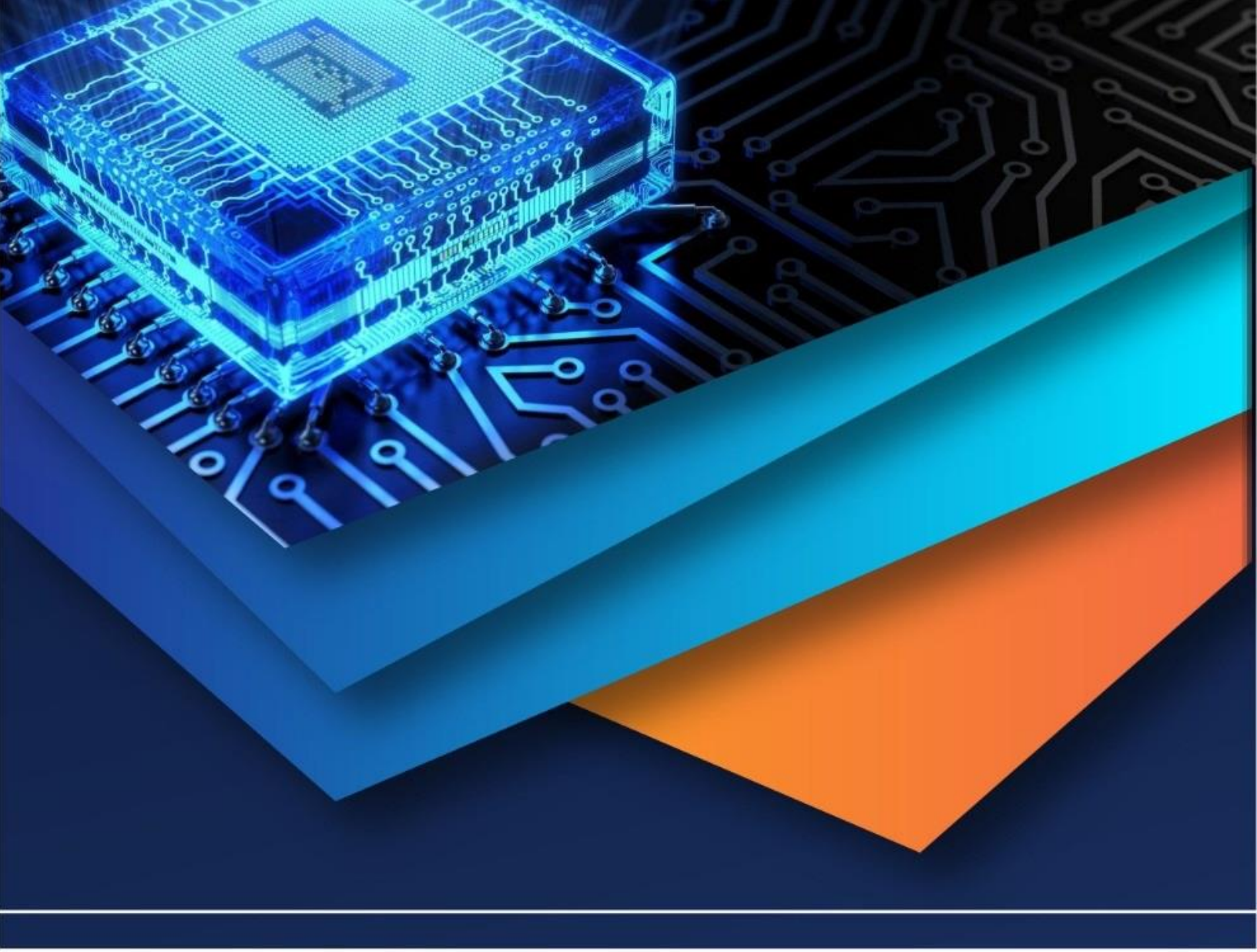
IV. CONCLUSION

Social networks have become part of our life and on average most internet users spend more time on social networks. In this paper we have presented a scenario which scares social network users and can imperil their identities and privacy. Furthermore we have provided examples of presented threats that are real and endanger every user. We have also emphasized certain threats which challenge the safety of young children across social network cyberspace.

REFERENCES

[1] Facebook, http://www.facebook.com/, [Online; accessed 14-January2014].
[2] Google+, https://plus.google.com/, [Online; accessed 14-January2014].
[3] LinkedIn, http://www.linkedin.com/, [Online; accessed 14-January2014].
[4] Sina Weibo, http://www.weibo.com/, [Online; accessed 14-January2014].
[5] Twitter, http://www.twitter.com/, [Online; accessed 14-January-2014].
[6] Tumblr, http://www.tumblr.com/, [Online; accessed 14-January-2014].
[7] VKontakte, http://www.vk.com/, [Online; accessed 14-January-2014].
[8] Facebook, "Facebook reports fourth quarter and full year 2013 results," http://investor.fb.com/releasedetail.cfm?ReleaseID=821954, 2014, [Online; accessed 24-February-2014].
[9] J. Feinberg, http://www.wordle.net/, [Online; accessed 14-January2014].
[10] Wikipedia, "List of virtual communities with more than 100 million active users," http://en.wikipedia.org/wiki/List of virtual communities with more than 100 million active users, [Online; accessed 08-September-2013].
[11] Facebook, "Form 10-k (annaul report) - filed 02/01/13 for the period ending 12/31/12," http://files.shareholder.com/downloads/AMDANJ5DZ/2301311196x0xS1326801-13-3/1326801/1326801-13-3.pdf, 2013, [Online; accessed 09-January-2014].
[12] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbot network: when bots socialize for fame and money," in Proceedings of the 27th Annual Computer Security Applications Conference. ACM, 2011, pp. 93–102.

[13] A. Mislove, B. Viswanath, K. Gummadi, and P. Druschel, "You are who you know: Inferring user profiles in online social networks," in Proceedings of the third ACM international conference on Web search and data mining. ACM, 2010, pp. 251–260.
[14] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks," in Proceedings of the 18th international conference on World wide web. ACM, 2009, pp. 551–560.
[15] J. Baltazar, J. Costoya, and R. Flores, "The real face of koobface: The largest web 2.0 botnet explained," Trend Micro Research, vol. 5, no. 9, p. 10, 2009.
[16] Q. Cao, M. Sirivianos, X. Yang, and T. Pregueiro, "Aiding the detection of fake accounts in large scale social online services," in Proceedings of the 9th USENIX Conference on Networked Systems Design and Implementation, ser. NSDI'12. Berkeley, CA, USA: USENIX Association, 2012, pp. 15–15. [Online]. Available: http://dl.acm.org/citation.cfm?id=2228298.2228319.
[17] G. Stringhini, G. Wang, M. Egele, C. Kruegel, G. Vigna, H. Zheng, and B. Y. Zhao, "Follow the green: growth and dynamics in twitter follower markets," in Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013, pp. 163–176.
[18] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of a social botnet," Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 57, no. 2, pp. 556–578, 2013. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2012.06.006
[19] A. Elyashar, M. Fire, D. Kagan, and Y. Elovici, "Organizational intrusion: Organization mining using socialbots," in International Cyber Security Conference. IEEE/ASE, 2012.
[20] J. Wolak, D. Finkelhor, K. Mitchell, and M. Ybarra, "Online "predators" and their victims," Psychology of Violence, vol. 1, pp. 13–35, 2010.
[21] 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, 2008.
[22] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of facebook and myspace," in Proceedings of the Thirteenth Americas Conference on Information Systems (AMCIS 2007), 2007, paper 339. [Online]. Available: http://aisel.aisnet.org/amcis2007/339/
[23] MySpace, http://www.myspace.com, [Online; accessed 14-January2014].
[24] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in Privacy enhancing technologies. Springer, 2006, pp. 36–58.
[25] C. Tucker, "Social networks, personalized advertising, and perceptions of privacy control," in Proceedings of the Tenth Workshop on the Economics of Information Security (WEIS), 2011.
[26] C. C. Miller, "Tech companies concede to surveillance program," The New York Times, June 2013, http://www.nytimes.com/2013/ 06/08/technology/tech-companies-bristling-concede-to-governmentsurveillance-efforts.html [Online; accessed 14-January-2014].
[27] C. Jernigan and B. F. Mistree, "Gaydar: Facebook friendships expose sexual orientation," First Monday, vol. 14, no. 10, 2009.
[28] M. Kosinski, D. Stillwell, and T. Graepel, "Private traits and attributes are predictable from digital records of human behavior," Proceedings of the National Academy of Sciences, vol. 110, no. 15, pp. 5802–5805, 2013.
[29] Facebook, "Facebook newsroom," http://newsroom.fb.com/Key-Facts, 2013, [Online; accessed 14-January-2014].
[30] J. Brenner and S. Aaron, "72% of online adults are social networking site users," http://pewinternet.org/Reports/2013/social-networkingsites/Findings.aspx, August 2013, [Online; accessed 9-January-2014].



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY