International Journal of Management, IT & Engineering
Vol. 9 Issue 6, June 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

STUDY OF SECURITY VULNERABILITIES IN SOCIAL NETWORKING WEBSITES

Rakhi Sunhare[*]

Dr.YasminShaikh[*]

Keywords:

Security;

Social Networking Websites;

Vulnerability;

Cyber crime;

Abstract

Social networking Websites (SNW's) have billions of active users who communicate and share their personal and business related information every day. The growing popularity of these websites has become a favorite place for attackers. Attackers use the SNW's vulnerabilities to access users' personal or business information. Vulnerability is weakness or flaw in the social network infrastructure which can be used by an attacker to harm the system, access the information, disturb its normal operations and use it for own financial or competitive benefits of for criminal activities crime or other motives. The main objective of this paper is to describe network and privacy related SNWs vulnerabilities. The vulnerabilities that are mainly used attackers are also highlighted in this paper. The paper presents a broad view of SNWs vulnerabilities to the researchers who are interested in improving security measures of social media services.

[*] **Pursuing Ph. D. In Computer Science, International Institute of Professional Studies (IIPS) ,Devi Ahilya University (DAVV), Indore (M.P.), INDIA**

I. INTRODUCTION

In the present day world of Internet millions of users regularly visit thousands of Social Networking Websites (SNW's). SNWs have become one of the most important communication channels between various kinds of service providers and clients on the Internet. The SNWs allow users to create posts and share them, share images, videos, activities, backgrounds, chatting and scarping, to connect through Internet. With the increasing use of Internet, millions of people have started using the SNW's for communicating with their business members, office staffs, relatives, friends, partners, family members, etc. [1]. According to statistical reports, almost 4.2 billion people were active internet users and over 3.4 billion Internet users have accessed various SNW's in 2018. China, India and the United States ranked ahead of all other countries in terms of internet users [2]. Figure.-1, show the number of SNW users in India.

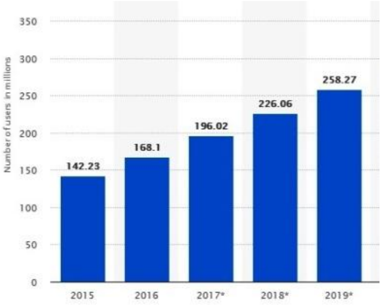

Figure 1: Number of SNW's users in India [2].

SNWs have large databases of users like: user activities, interest, information about user's profession, financial information, personal photos/videos, email addresses, Internet Service Provider's information, and some have authorized location tracking. Attackers and cyber criminals steal this type of information through SNWs vulnerability and can potentially use it against users.

Vulnerability is a security term that refers to a flaw in a SNWs that can leave it open to attack. There are several types of vulnerabilities that users may encounter. Vulnerabilities cause a disruption in the integrity, confidentiality availability, authorization and authentication of services. Criminals or attackers can use these vulnerabilities to commit crime against social media users. Social media affect almost each and every part of our society; like individuals, businesses, and government. Unfortunately, some of these effects have negative impact and bring new versions of violations and crimes.

The rest of the paper is arranged as follows. In Section II, related work is presented, in Section III, some popular SNW’s are described, In Section IV, SNWs vulnerabilities are categorized. Last section includes discussion and conclusions.

II. RELATED WORK

With the huge growth of SNWs, several researchers have highlighted security issues due to vulnerabilities in SNWs. Number of users of SNW’s is increasing day by day and as a result huge amount of data is getting accumulated [3]. Attackers are also increasing to gain access over sensitive information of other users. Hacked information can be used in so many ways. SNW’s such as Facebook, Twitter, Myspace, Google+, and LinkedIn are popular social websites. The growing popularity of these websites has become a target for crime and attacks. According to a survey report, Facebook needs, improvement of default privacy setting to prevent attacks and disclosure of personal information publicly [4].

Apart from this still many other features need to be improved for enhancing privacy and security of SNW’s. At the same time, the media being the fourth pillar of democracy should play a positive role by creating social awareness amongst the people about the careful use of SNW’s and thereby not falling prey to crime [5].

An analysis says that 78.9% of the threats that actuate the social media networks are not actually security faults rather they prey on the user’s lack of knowledge on handling computer systems and traversing the internet [6]. By deceiving such users and making them click on malicious links and download malicious code they breach the privacy of these users. Although companies like Google and Facebook use complex machine learning algorithms for spam detection, they also have an about 5% chance of not being able to detect spam. By educating users of spam emails and phishing, 70% of threats can be negated.

The use of social media has been increasing rapidly, and therefore has become a breeding ground for both online criminals and terrorist activities [7]. Many harmful crimes occur through social media such as blackmailing, terrorist propaganda, online fraud, therefore there is an urgent need to combat them. The use of information is increasing everyday with the advent of more applications of social media platform that utilizes voluminous data per second globally [8]. These data include sensitive information such as trade secret, privacy and security issues. Attacker use this opportunity to launch more attacks by attacking people's privacy and steal sensitive information such as credit card details, online shopping information of customers, online ticket booking. The increasing use of SNW’s has lifted concerns about the misuse of people's privacy. Online networking websites like Twitter, Facebook, LinkedIn, etc. are the most popular websites for information sharing among users and it is understandable that business organizations use the information from SNWs. However, it is necessary that the information that is found on SNW is not misused [9]. The service provider like Facebook should be aware of data miners who may try to attack people’s privacy [10].

Any improper privacy policy of the SNW can increase the chance of privacy attack. The privacy of people is determined by the user’s characteristics and their use of SNW [11]. The research has confirmed that due to different cultural differences in many countries, people tend to be more conscious and less conscious in disclosing their private information in SNW. The modest part of privacy is, the attack done by hackers to determine the behavior of people and using their information against them. In social networking, personal information can be acquired by anybody, anytime, anywhere through the Internet [12]. SNWs allow users to message and post their feelings, share experience and more interesting personal information. There are many issues regarding security within such environment. Several security vulnerabilities and threats associated with Facebook are explored.

The social media networks allow free communication between their users and the possibility to create new and positive links; however, this freedom of communication also creates conditions for abuse [13]. Nowadays, the users on SNWs share everything about their private lives online leading to rise in misuse of personal information through social media networks. Thus, it suits every person to measure the risks well, which is far from being evident, if we consider the numerous affairs in which users become victims. In this free space, one meets not only friends, but also people who might belong to organized networks searching for vulnerable targets – and in particular children [13]. In [14], the author focused on how personal information is being affected by the internet and social media, discussed how the privacy becomes a risk and how to assign security awareness to prevent security breaches. The current situations of using social network and threats that can affect the users are also highlighted in the article. Finally, some security awareness that can be practiced to be more aware of social network threats is presented.

SNWs allow users to share information, views with unknown and can connect well with recognized friends [15]. Hackers without much of stress get into and assemble their own and delicate data. Users are less aware and minimum worried about the security setting. The social networking websites needs to be focus on the protection of user's personal information's.

III. POPULAR SOCIAL NETWORKING WEBSITES

The top SNW's are commonly available in multiple languages and allow users to connect with friends or people across geographical, political or economic borders. Facebook was the first SNW to surpass 1 billion monthly active users. Following are the main SNW's that are popular among the users [2, 16-22]:

A. Facebook**:** Facebook has now become the most popular and widely used SNW. Using Facebook one can communicate with others, share thoughts or views, make friends, upload photos or tag photos, share a common interest, can create pages, like pages, join groups and many more. According to the Statistics Portal, 2.94 billion users are using Facebook in India and overall world as of the third quarter of 2018, Facebook has over 2.2 billion monthly active users.

B. Twitter**:** Twitter was founded by Jack Dorsey, Biz Stone and Evan Williams in March of 2006. Twitter is a micro blog service. At the beginning of 2019, it held more than 1.3 billion registered users. Close to 460,000 new Twitter accounts are registered every day. Each user can post short messages of up to 140 characters on his or her account. Other users can then subscribe or follow that person's page and receive their update messages. In the third quarter of 2018, Twitter had 330 million active users in worldwide and 7.83 million active users in India. According to dustn.tv, twitter has over 330 million monthly active users.

C. YouTube**:** YouTube allows users to upload, view, rate, share, add to favorites, report, comment on videos, and subscribe to other users. Anyone can like, view, share, comment on the videos posted by anyone. It is one of the SNW, which also helps the user to earn money through uploading videos. In YouTube monthly user base touches 225 million in India. YouTube has over 1.5 billion monthly active users.

D. Google+: Google Plus is a social network owned by Google. It was launched in 2011 and was meant to be a social layer across all Google's products. There are approximately 395 million monthly active users on Google+. Google+ is estimated to have over 2 billion registered users worldwide. Google+ has over approximately 395 million monthly active users.

***E. LinkedIn*:** This SNW's helps business people to share their work related information with each other and with their clients. LinkedIn is the world largest professional SNW with more than 562 million users in more than 200 countries and territories in worldwide. According to the Statistics Portal, 52 million users are using LinkedIn in Indian. LinkedIn has over 200 million monthly active users.

F. Instagram: Instagram is a photo and video sharing social networking service owned by Facebook. According to the Statistics Portal, 71 billion users are using Instagram in Indian and overall world as of the third quarter of 2018. Instagram has over 800 million monthly active users.

IV. CATEGORIZATION OF VULNERABILITIES IN SOCIAL NETWORKING WEBSITES

The SNW's vulnerabilities can be categorized into two categories- First is social network related vulnerabilities and second is privacy related vulnerabilities. A brief description of each category of security vulnerabilities is presented here.

1. *Social Network Related Vulnerabilities:*

Social network related vulnerabilities are related to either with the security of the people or with the safety of the data that is stored in the social network server or cloud. There are some attackers or hackers who use social network vulnerabilities to steal the information of different active users and then use this information for their own benefit. Some social network related vulnerabilities are: Data Leaks, Shortening, Fake Profiles, Sybil, Click-jacking, Cross-Site

Request Forgery and Cross Site Scripting, and Identity theft. Some social network related vulnerabilities are [23-27]:

1.1. ***Cross-Site Request Forgery and Cross Site Scripting:*** Cross-Site Request Forgery and Cross Site Scripting Vulnerability occurs when a malicious website, email, blog or program, opened on a user's computer, uses the user's browser to initiate connectivity to another website, and then uses login of the unsuspecting user to carry out malicious attack on the website it has connected. So as long as the social network websites are not checking the referrer header, it's easy for an attacker to share an image in a user's event stream that other users might click on to catch or spread the attack.

1.2. ***Data Leaks*:** Social networks are all about sharing information. Unfortunately, many users share a bit too much about the organization, project, products, financials, organizational changes, scandals, or other sensitive information. Social networking provides a significant unprotected channel for data leaks, it incents people to over-share confidential information, it provides hackers with information that greatly assists them in breaching organizations, and it allows the dissemination of lies in the form of misinformation or impersonation. The resulting issues include the embarrassing, the damaging and the legal.

1.3. ***Sybil:*** Sybil attacks can look a great deal like identical cloning. However, in a Sybil attack, the attacker is not stealing the identity of another user; he or she is making multiple profiles instead. Each identity that a Sybil attack creates has a direct node attached to it. By having the multiple profiles, one can influence the choices made by victims' friends using the trust built on friendships. An attacker can use the identities to launch malicious messages and spam other users.

1.4. **Click-jacking:** Numerous click-jacking scams have employed "Like" and "Share" buttons on SNW. Disable scripting and frames in whatever Internet browser you use. Research other ways to set your browser options to maximize security.

1.5. ***Fake Profiles*:** In SNW user can also apply some privacy settings to keep their data private but the attacker can get the personal information provided by the user and use them to create fake profiles. Fake profiles are a risk that can be very serious because it has been used by sexual offenders, people meaning to defame or harm other users. By manipulating fake profile, first the criminals or hacker builds friendship with the friends of the victim and later will steal the personal information and misuse in other crimes.

1.6. ***Content Sniffing XSS Vulnerability:* I**t is a very dangerous form of vulnerability as the embedded malicious code will surely run on the certain SNWs according to the JavaScript's original policy. In Content-Sniffing XSS attack, an attacker carefully embeds HTML code containing JavaScript code into a non-HTML file and uploads this file to an honest website. By this way, the attacker let the user to run that malicious code in his/her browser.

2. *Privacy Related Vulnerabilities:* In past few years the uses & users of SNW's are increasing speedily. This increase in the number of users has paved a new way for the attackers to access user information. Privacy related vulnerabilities can be faced due to posting and sharing on of personal information on SNWs. SNW users post and share a lots of personal and professional information while creating profile such as profession details, business details, addresses, mobile numbers, date of birth, anniversary date, hobbies, and so on. Attackers can use this information for social engineering. The social engineering is a way of committing a crime using Vulnerabilities. Few Privacy Related Vulnerabilities are discussed here [28-34]:

2.1. ***Information Leak/ Privacy Conflict***: Information leak means the information available on user's profiles is accessed by someone else and the same information is hsed for malicious activities or frauds. SNW users openly share and exchange personal information with their relatives, friends, family and other users in the social network. Personal information leak means user's personal information is disclosed to unwanted persons without that user's consent.

2.2. ***Identity theft:*** Identity theft is a real and serious problem in our country as well as other countries. It succeeds with minimal key information. It is a form of stealing someone's personal information such as name, profile picture, place, date of birth, address etc. without the knowledge of that person and then use it to create another account or commit crime such as fraud or theft.

2.3. *Malicious Crawlers:* The availability of personally sensitive information present in user profile makes attackers more interested in perpetrating more attacks on SNWs. Crawlers are automated software which have the ability to access and download large amount of user's information's on SNWs. Automated crawlers are challenges to the today's security measures. Using this vulnerability criminal steal and misuse large amount of users' personal information.

2.4. *Stealing passwords and phishing:* Passwords are used as a mean for identification of users on social networks, it is sufficient for a hacker to know the sequence of characters. Once the hacker know the password, he/she can to send advertising, some information on behalf of others, or to motivate recipients to take any negative action, in particular to pass on the link and run the malicious code, and do other (often illegal) activities. Besides, some companies use social network to promote their own products, and the theft of an administrator group password allows stealing the group itself. To obtain confidential information traditionally, phishing, dummy websites, social engineering, are used. Protection against these attacking methods is considered DLP-system (Data Loss Prevention-system) and reputation technologies that are integrated into a variety of anti-virus products.

2.5. *Profile cloning:* Profile cloning is a very harmful type of attack. Profile cloning, also known as identity cloning, is commonly seen on SNWs. Profile cloning attacks can be classified into two types, same-site and cross-site profile cloning. In same-site profile cloning, an attacker creates cloned profiles in a particular SNW that mimic the victims profile in the same SNW. In cross-site profile cloning, the victim's personal information is taken from one SNW and misused by an attacker in different SNWs in which he or she does not have accounts.

2.6. *Social Engineering:* Social networks allow attackers to find confidential information that can be used for personal and moral damages. Social engineering is a type of vulnerability which is an art of cheating someone's confidential information with the ways that the victims never notice that their confidential information is stolen and used to committing a crime or for any financial benefit of adversary.

2.7. *Phishing Attacks:* Phishing attacks are a form of social engineering to acquire user-sensitive and private information by impersonating a trustworthy third party. It is a common threat on the SNWs in which the attacker or criminals creates and controls a fake website that looks like a legitimate one to lure victims into entering sensitive information.

2.8. *Weak or default Passwords*: Many SNWs, content management systems, and even database servers are still configured with weak or default passwords. Having a weak password, cyber criminal easily breaks the database passwords and access the all information is stored in databases.

Vulnerabilities cause a disruption in the integrity, confidentiality, availability, authorization and authentication of social media services. Following table shows the vulnerability impact on the security goals.

Table 1: Vulnerability Impact on Security Goals

No	**Major Security Vulnerability**	**Vulnerabilities Impacts on the Major Security Goals**				
		Availability	**Confidentiality**	**Integrity**	**Authentication**	**Authorization**
1	Cross Site Scripting/ Cross-Site Request Forgery	-	✓	-	✓	✓
2	Data Leaks	-	✓	✓	-	✓
3	Sybil	✓	✓	✓	✓	-
4	Click-jacking	-	✓	-	-	-
5	Fake Profiles	✓	✓	-	✓	-
6	Content Sniffing XSS Vulnerability	-	✓	-	✓	✓
7	Information Leakage/ Privacy Conflict	✓	✓	✓	-	✓
8	Identity theft	✓	✓	✓	✓	✓

9	Malicious Crawlers	✓	✓	-	-	✓
10	Stealing passwords and phishing	-	✓	-	✓	-
11	Profile cloning	-	✓	✓	-	✓
12	Social Engineering	-	✓	✓	✓	✓
13	Phishing	-	✓	-	✓	✓
14	Weak or default Passwords	-	✓	✓	-	-

V. CONCLUSIONS

The uses of SNW's are increasing day by day. The status of website, namely Facebook (2.2 billion monthly active users), LinkedIn (200 million monthly active users), YouTube (1.5 billion monthly active users), Google+ (approximately 395 million monthly active users), Instagram (800 million monthly active users and Twitter (330 million monthly active users) has made communication for people and interact with anybody making use of Internet in a few seconds. But the largest collection of personal and professional data found in SNW's shared by users probing for crimes. This paper contributes to research by providing a broad overview of social network and privacy related vulnerabilities faced by users when using SNWs. The vulnerabilities impacts on major security goals are also discussed in the paper.

This paper presents a broad view of privacy related vulnerabilities and shows social engineering vulnerabilities are the most important challenges in SNW's. The paper also highlights the need to improve the privacy measures of social media services. At the same time, it is suggested that there is a need to develop tools or techniques that can automatically detect and report crime committed by using social engineering vulnerabilities.

REFERENCES

[1]. Y. Najaflou, B. Jedari, F. Xia, L. T. Yang and M. S. Obaidat, "Safety Challenges and Solutions in Mobile Social Networks," in IEEE Systems Journal, Vol. 9, No. 3, pp. 834-854, Sept. 2015.

[2]. https://www.statista.com/statistics

[3]. Seema D. Trivedi et al, "Analytical Study of Cyber Threats In Social Networking," International Conference on Computer Science Networks and Information Technology, vol. 3, no. 2, pp. 32-36, 2016.

[4]. RoshanJabee et al, Issues and Challenges of Cyber Security for Social Networking Sites (Facebook), International Journal of Computer Applications, Volume 144 – No.3, pp-36-40, June 2016.

[5]. Dr. RekhaPahuja, Impact of Social Networking on Cyber Crimes: A Study, Epitome-International Journal of Multidisciplinary Research, Vol. 4, Issue 4, pp-9-14, April 2018.

[6]. Sanyuj Singh Gupta et al, Social Media Security, International Conference on Advances in Computing and Communication Engineering (ICACCE-2018) Paris@2018-IEEE, pp-115-120, Year-2018.

[7]. Faisal YousifAlanezi, Social Media as A Tool for Combating Cybercrimes With Special Reference to Saudi Arabia, Asia Pacific Journal of Advanced Business and Social Studies, Volume 2 Issue 2, pp-610-624, Year-2016.

[8]. Ibrahim AbdulaiSawaneh, Examining the Effects and Challenges of Cybercrime and Cyber Security Within the Cyberspace of Sierra Leone, International Journal of Intelligent Information Systems, 7(3), pp-23-27, Year-2018.

[9]. AmritRegmi, Impact of Privacy Invasion in Social Network Sites, IEEE, pp-457-462, Year-2018.

[10]. J., Gerlach et al,"Handle with care: How online social network providers' privacy policies impact users' information sharing behavior", Journal of Strategic Information Systems, Vol. 24, pp. 33-43, Year-2015.

[11]. C. Park et al, "Consumer characteristics and the use of social networking sites", International Marketing Review, 32(3/4), 414437, Year-2015.

[12]. M. Ganesanet. al, Cyber Crime Analysis in Social Media Using Data Mining Technique, International Journal of Pure and Applied Mathematics Volume 116 No. 22, pp-413-424, Year-2017.

[13]. S. Leitch et al, and Warren M. Security Issues Challenging Facebook, Proceedings of the 7th Australian Information Security Management Conference, pp-137-142, Year-2009.

[14]. RoshanJabee et al, Issues and Challenges of Cyber Security for Social Networking Sites (Facebook), International Journal of Computer Applications, Volume 144 – No.3, pp-36-40, June 2016.

[15]. Faisal YousifAlanezi, Social Media as a Tool For Combating Cybercrimes With Special Reference To Saudi Arabia, Asia Pacific Journal of Advanced Business and Social Studies, Volume 2 Issue 2, pp-610-624, Year-2016.

[16]. http://m.facebook.com

[17]. http://myspace.com

[18]. http://www.orkut.com

[19]. http://blog.twitter.com/2010/02/measuring tweets.html

[20]. https://dustn.tv/social-media-statistics

[21]. Seema D. Trivedi et al, "Analytical Study of Cyber Threats In Social Networking," International Conference on Computer Science Networks and Information Technology, vol. 3, no. 2, pp. 32-36, 2016.

[22]. https://dustn.tv/social-media-statistics

[23]. M. Sreenu et al, A General Study on Cyber-Attacks on Social Networks, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 19, Issue 5, PP 01-04, Year-2017.

[24]. Lei Jin et al, Sybil Attacks VS Identity Clone Attacks in Online Social Networks, School of Information Sciences University of Pittsburgh, Pittsburgh, PA, USA, pp-125-127.

[25]. Dr. N. Jayalakshmi et al, PRIVACY IN SOCIAL NETWORKING WEBSITES, International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 09, pp. 2109-2113, Dec-2015.

[26]. Mauro Conti et al, FakeBook: Detecting Fake Profiles in On-line Social Networks, IEEE, pp. 1071-1078, 2012.

[27]. MisganawTadesseGebre et al, A robust defense against content-sniffing xss attacks. International Conference on Digital Content, Multimedia Technology and its Applications (IDC). pp. 315-320

[28]. S. Unnikrishnan et al, Security Issues of Online Social Networks, Springer-Verlag Berlin Heidelberg, ICAC3 2013, CCIS 361, pp. 740–746, 2013.

[29]. Sri KhetwatSaritha et al, Link Encryption to Counteract with Rouge Social Network Crawlers, Ninth International Conference on Information Technology- New Generations, IEEE, pp. 83-84, 2012.

[30]. Algarni et al, Social Engineering in Social Networking Sites: The Art of Impersonation. IEEE International Conference on Services Computing (SCC). pp. 797-804, 2014.

[31]. Jin, L. et al, Towards active detection of identity clone attacks on online social networks. Proceedings of the first ACM conference on Data and application security and privacy, ACM. pp. 27-38, 2011.

[32]. Samar Albladi et al, Vulnerability to social engineering in social networks: a proposed user-centric framework. In: 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF). IEEE, Piscataway, NJ, pp. 95-100, 2016.

[33]. M. Omar et al, "Threats and Anti-threats Strategies for Social Networking Websites," International Journal of Computer Networks & Communications, vol. 5, pp. 53-61, 2013.

[34]. Kristian Beckers et al, Analysis of Social Engineering Threats with Attack Graphs.

[35]. http://dictionary.cambridge.org