ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.4. No.2, Pages : 01-06 (2016)
Special Issue of ICCECT 2016 - Held at The Savera, Chenna, India
http://www.warse.org/IJETER/static/pdf/Issue/iccect2016sp01.pdf

A Survey on Threats and Vulnerabilities in on-line Social Networks

D.Santhana Lakshmi[1], Dr.T.Hemalatha ,ASP/CSE[2]

[1]Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul, India. Santhanalakshmi1993@gmail.com

[2]Department of Computer Science and Engineering PSNA College of Engineering and Technology, Dindigul, India. hemashek@yahoo.com

Abstract— Social Network is the technique that maps and measures the relationships and flows between people, groups, organization, computers, URL and information. The nodes in the network are the people and group while the link shows the relationship between the nodes. Social Networks facilitate the connections between people based on shared interest, values and group and then communication between the individuals becomes more easily using web as interface. According to the current status of the social networks, the usage of Facebook has increased day by day and currently 71% of online adults are using Facebook which has the huge popularity of 46.5%. In spite of the higher usage, popularity and demand there are several challenges and threats. There are several threats in social networks, which include Classical threats, Modern threats, Combination threats, Threats targeting children, etc. In this work the following threats Identity clone attacks, Socware, Cyber bullying, is considered for which prevention strategies will be undertaken. Identity Clone Attack duplicates the user's online presence. Socware fakely damage the post and messages. Cyber bullying is dangerous with negative outcome to both bully and victim but which can be resolved through the proposed system. The objective of the proposed system is to stop cyber bullying by which Combination threats and Clone attack can also be eliminated.

Keywords—Online social networks, security and privacy control , social network security solutions.

INTRODUCTION

A social network service as a service which ―Cornerstone on building and verification of online social networks for communities who wish share interests and activities, or who are interested in exploring the interests" [3]. Social networks can provide huge benefits to members of an organization such as, **Support for learning**: Social networks can improve informal learning with the support for the social connections.

Support for members of an organization: Social networks can potentially be used by all members of an organization, and not just elaborating the working with all students. Social networks can help in the improvement of communities of practice. **Engaging with others**: Passive use of social networks will benefit us to provide valuable business intelligence and feedback on institutional services. **Ease of access to information and applications**: With the ease of use of many social networking services can provide benefits to users by simplifying access with the built-in tools and applications. The Face book Platform illustrates an example to show how a social networking service can be worn as an environment for other tools. **Common interface**: A manageable convenience of social networks may be the common interface which extends the work of social boundaries. Since such services are often used with a personal capacity interface and then the service works to be familiar, thus minimizing training and support needed to make use of the services in a professional context.

ONLINE SOCIAL NETWORK USAGE

In recent years many OSNs have tens millions of registered users. Among that Facebook is in the leading position, with more than billions of active users, and it is most desired OSN in the world. Then the Other well-known OSNs are Google+, Twitter, and LinkedIn with more than 235, 200 160 million active users respectively. While some experts insist that OSNs are a passing fashion but it stays due to the current user statistics and will eventually be replaced by another Internet fad, According to the recent survey made by the Pew Research Center's Internet and American Life Project disclosed that 72% of online American adults use social networking sites, there is a dramatic increase from the 2005. Pew survey statistics shows that just only 8% of online adults used social networking sites. According to the Fig 1 the survey disclosed that 89% of online adult's ages are between 18 to 29 use social network sites, but in 2005 only 9% of the adults use this type of sites. The statistics survey results of previous years have no conflict with recent years are published by Nielsen in 2011.

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.4. No.2, Pages : 01-06 (2016)
Special Issue of ICCECT 2016 - Held at The Savera, Chenna, India
http://www.warse.org/IJETER/static/pdf/Issue/iccect2016sp01.pdf

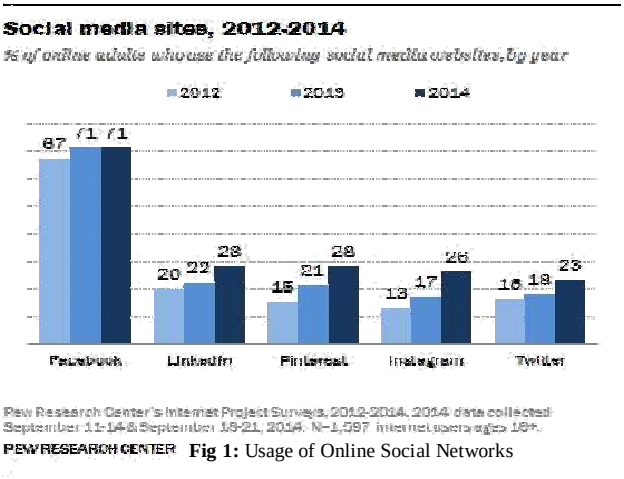

Fig 1: Usage of Online Social Networks

As revealed in the Fig 2 that the users spent 22.5% of their online presence on OSNs and blogs, more than twice the time spent on online games (9.8%).The Collective time spent on different online sites which includes electronic-mail (7.6%), portals (4.5%), videos and audios (4.4%), searching events (4.0%), and instant messaging (3.3%). Among the different strategies the amount of time spent on OSNs, especially on Facebook is immense, fast and ever-growing [13].

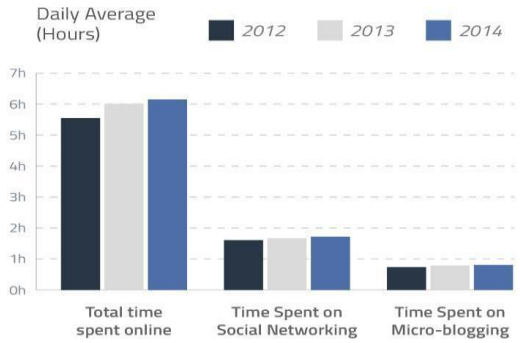

Fig 2: Users Average Time Spent on Online Sites

According to December 2013 survey results, Facebook had approximately 556 million daily active mobile users, which would made a gradual increase of 49% year over year. Additionally, Facebook and Google+ are most frequently used smartphone applications [13]. So it is notable that the use of OSNs on mobile devices not only promotes a ―closer relationship‖ to social networks but also can create and pose additional privacy concerns, regarding the collection of data to specific types of users.

Table 1: Popularity of Social Networks

Social Networks	2015
Face book	46.5%
Twitter	4.58%
Instagram	1.23%
LinkedIn	1.33%
Yahoo	1.28%
Google Plus	1.28%

According to the Table 1 statistics, the popularity of the OSN is not only among the adults, but also it is extremely popular with young children and teenagers. That is Overall 60% of children 9 to 16 years old who make daily access to the Internet for about 88 minutes approximately. Among this 26% of ages is from 9 to 10; 49% of ages 11 to 12; 73% of ages 13 to 14 and82% of ages 15 to 16. Users under age of 13 are not officially allowed to use OSN. Additionally, 30% survey reported that the children having a facebook connection with a person whom they have never met face to face so far, only 9% reported having actually met face to face with someone with whom they had only an facebook connection. 21% of the survey results in harmful user-generated content [14].

The usage of OSNs is incorporated in the everyday lives of young children and teenagers; this may result in personal information being revealed, misused, and potentially abused.

ANALYSIS OF THE EXISTING SYSTEM

Recent trend had made the users to upload the pictures of themselves and their friends. Facebook records about billions of photos everyday [10]. Network security is a major part of the network that is needed to be maintained because information is passed between the computers and is vulnerable to attacks. A threat is a possible danger that might exploit vulnerability to breach all security settings and thus cause possible harm. Threats can lead to attacks on computer systems, networks and more.With the increasing amount of people getting connected to the networks the security threats that cause a massive harm are also increasing. These threats can be divided into four categories. The first category contains classical threats, security threats not only attack the personal information but also accomodating to that particular environment (see Section III-A). The second category includes modern threats, threats that create a fake profile and then view and attack that particular profile (see Section III-B). The third category consists of combination threats, attackers today combine various types of attack to create more sophisticated and legal attacks (see Section III-C). The fourth category includes threats specifically targeting the children who use the social networks (see Section III-D)

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.4. No.2, Pages : 01-06 (2016)
Special Issue of ICCECT 2016 - Held at The Savera, Chenna, India
http://www.warse.org/IJETER/static/pdf/Issue/iccect2016sp01.pdf

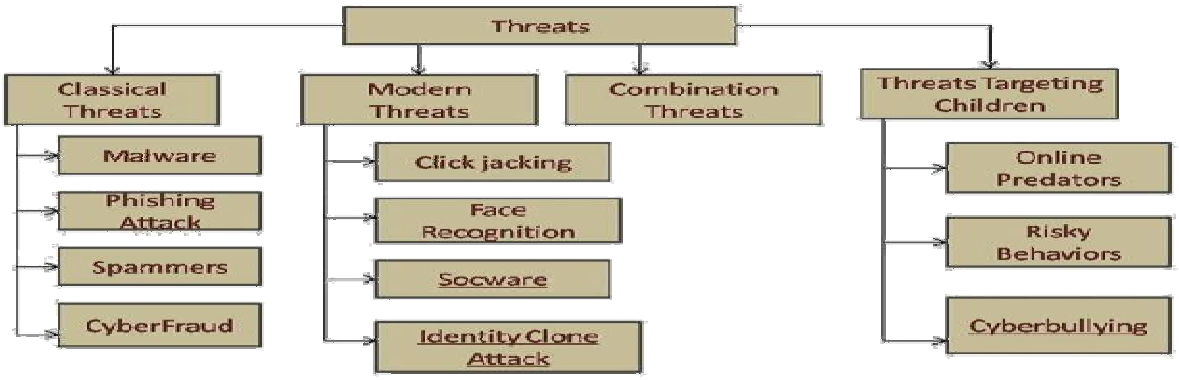

Fig 3: Threats to online social network users

Categories of Threats

A. Classical Threats

Classic threats can take a user's personal information published in an OSN and make harm only the user but also their friends by adjusting the threats to accommodate to that user's personal information. The innocent user will open the message and getting infected is likely. Most of the threats, target everyday user resources such as credit card numbers, account passwords. These types of threats can also exploit the infected user's stolen credentials or to post messages on the user's behalf by simply changing the user's personal information [7].

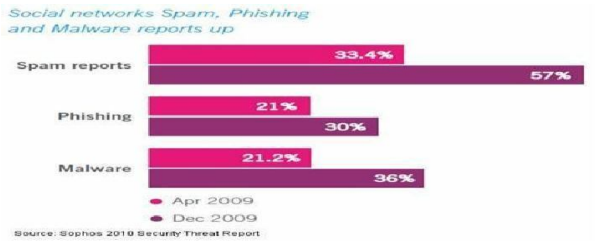

Fig 4: Malware, Phishing Attack and Spammers attack in Social Networks

With the reference to the Fig 4 different classic threats are described below, Malware: Malware is malicious code developed to disrupt a computer operation in order to collect a user's credentials so that he can gain access to his or her private information. Phishing Attacks: Phishing attacks are a form of attack used to acquire user-sensitive and private information by pretending to be a trustworthy third party. According to the recent statistics phishing attacks have been increased rapidly report 84.5% of all phishing attacks target online social network site users is shown in Fig 5.

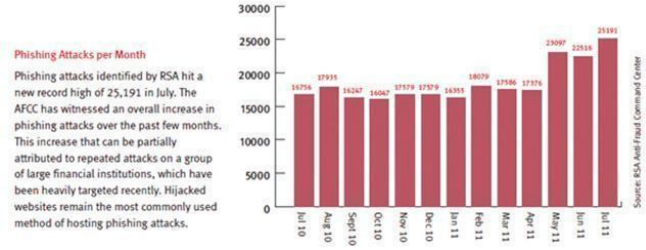

Fig 5: Survey Report of Phishing Attack

Spammers: Spammers use the electronic mailing system to send unwanted message to other users which is done by creating a fake profile [12]. According to the spam rate in different zone which is referred as Fig 6, 11% of Twitter messages were spam messages. But drastically it has been reduced to 1% [10].

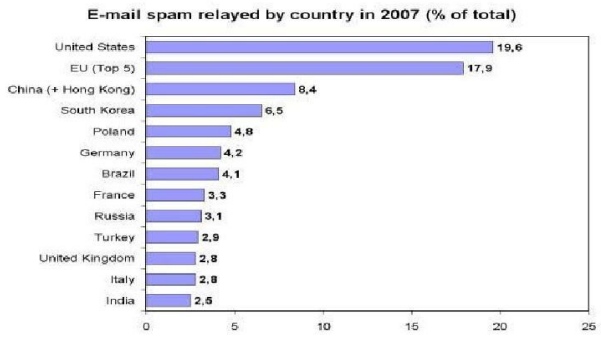

Fig 6: Spam Rate in different Zones

Cyber Fraud: Cyber fraud also referred to as internet fraud that takes advantage of people [15]. In recent survey, for example, fraud made the hacking into the accounts of Facebook.

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.4. No.2, Pages : 01-06 (2016)
Special Issue of ICCECT 2016 - Held at The Savera, Chenna, India
http://www.warse.org/IJETER/static/pdf/Issue/iccect2016sp01.pdf

Modern threats also target on the users as well as friends personal information and these threats are unique to the OSN environments .These threats create the fake profile, viewing the particular profile and then attacking that. This leads to the chain attack that the attacker can collect data from the user's facebook friends by inferring the high school.

Clickjacking: Clickjacking is a dangerous technique in which the intention of clicking something, hijacks the information from the source to the attackers. In case if the information contains sensitive data it will create a severe vulnerability to the users account. Further, an attacker can maliciously post spam messages as well as ―likes‖ is clicked to links unknowingly. This kind of attack is called likejacking [14].

De-Anonymization Attacks: Attacks is also possible even users adapt to the anonymity by De-anonymization attacks which uses the technique such as tracking user cookies, network topology, and memberships of the users group to disclose the user's real identity. Noncoverage of user identities to the third parties is an example of de-anonymization which is demonstrated by Krishnamurthy and Wills [5].

Fake Profiles: Fake profiles that mimic human behaviors in OSN. In many cases, fake profiles are used to disclose and harvest users' personal data from social networks. By initiating friend requests to other users in the OSN, who often accept the requests, the socialbots is a technique that gathers user's private data which should be exposed only to the user's friends. A socialbot is defined as a piece of software that is designed to have a presence on the Internet—especially on social media [8].

Identity Clone Attacks: The attackers duplicate the online presence that is done either by the use of same or different networks. For example, Identity of the ―dearly departed‖ to get passports, credit card, car loans. With a just little basic information it can be easy for an identity clone to build reputation that they are imitating [3].

Inference Attacks: An Inference attack is used in OSNs to predict a user's personal, sensitive information that the user are not willing to disclose, such as religious affiliation or sexual orientation.

Information Leakage: Negative impacts in the social network are created mainly because of risks that happen due to the Leakage of sensitive and personal information. For example, leaking personal information, such as drinking habits, on OSNs may jeopardize future chances for career development [9].

Location Leakage: Location Status updates which leads to the share of private information. For example, Israel Hyman from Arizona tweeted that he was looking forward to his family vacation to St. Louis. He tweeted once again, when he had arrived in Missouri. When Hyman returned home, he discovered that his house had been burglarized [6].

possibly damaging posts and messages from friends in OSNs. If the applications inject the malicious code then that would easily assist in spreading socware. An example illustrate the real life incidents, that acts appear to be part of a growing destructive trend which police had not ever seen here before, but which have already took place in other cities across the country. But it was first carried out by an rapper a year ago but that had been recreated on the internet by teenagers bound onto cars, police cruisers, on displays visualizes inside grocery stores and elsewhere, leaving behind very costly damage. The Akron videos, which were still remind on the teen's Facebook page as of about 10:00 p.m. Wednesday, were removed by Thursday morning, but the police had not ever seen here before and made copies."It's expensive, not only for the police department, but also to repair this damage. The videos had also already caught the attention. From the videos police were able to detect three teenagers. Late Thursday afternoon they had arrested Alexander Beasley, 18, of Akron, who is responsible for accusing for the film and post the videos online and participating in the acts at Garfield High School. Beasley was charged criminal damage. A 17-year-old Garfield High school student was also arrested and charged with criminal damaging and criminal trespassing [4].

C. Combination Threats

For more sophisticated attacks the combination threats are made into use. For example, an attacker can use a phishing attack and clickjacking, clone and spam, etc together to perform some destructive tasks in online social networks.

D. Threats Targeting Children

Children, whether young children or teenagers, certainly experience classical and modern threats, specific threats target younger users of OSNs.

Online Predators: Online Predator pretends adult man to be a friend of the innocent boy or girl who refuses the actual meeting but collect the personal data which leads to the rape or kidnapping.

Risky Behaviors: Use of chat rooms for interaction with strangers, sexually explicit with the strangers and giving out private information and photos to the strangers [16].

Cyberbullying: Cyberbullying is bullying technique by which the person uses the strength or influence to harm those who are weaker than others. In the case of Catherine, she thought anything she said on the Internet was harmless. However, one day she found that while at talking on Facebook with a friend about another acquaintance she was being targeted by a teen and clearly had an aggressive view towards Catherine. But she thought nothing would be mattered in the future, but thinking the teen was mistaken and wrong. However, after few weeks, Catherine was physically attacked by the same individual and she was

ISSN 2347-3983

International Journal of Emerging Trends in Engineering Research, Vol.4. No.2, Pages : 01-06 (2016)
Special Issue of ICCECT 2016 - Held at The Savera, Chenna, India
http://www.warse.org/IJETER/static/pdf/Issue/iccect2016sp01.pdf

bleeding. She left the party with a cut above her eye, but when Catherine went to the hospital, it was found that she had facial bone fractures instead [2].

VULNERABILITY – COUNTER MEASURES

There are comprehensive varieties of countermeasures for the different types of threats. But in recent years, social network operator and academic researchers have tried and produced better response in dealing with these types of threats.

A. Social Network Operator Solutions

In activating safety measures to different users the user authentication mechanisms and applying user privacy settings is applied.

Authentication Mechanisms make sure that the registered or login account is not compromised by the user. Authentication mechanism involves OTP Generation and OTP validation so that based upon that validated OTP, users can perform the corresponding functions.

Security and Privacy Settings are implemented in many OSNs support variety of configurable user privacy settings that enable users to protect their personal data from other users or applications [11], [12]. These are the default settings in the facebook.

Internal Protection Mechanisms are implemented with the certain protection measures to defend against the malicious attacks and other types of the threats such as spammers, fake profiles.

Solution to threats that concentrate the children in which detection and prevention of the threats targeting on the children and report abuse to the networks administrators.

B. Academic Solutions

Solutions to detect and prevent various types of security attack.

Recommendations to Improve and change Privacy and Setting Interfaces to avoid the default settings in the facebook which would make the information publically available to all the users. This type of implementation recommended many of the other users to change their privacy settings accordingly [1].

Phishing Detection is done mostly by the identification of phishing URL sites and collection of the survey reports. Several anti phishing methods are used to detect and prevent phishing attacks; most of these methods are based on techniques that attempt to identify phishing websites and phishing URLs [16].

Spammer threats is detected and recovered from that attack by collecting the spammer detection attacks that occurs before.

Cloned Profile Detection is a prototype of the implementation technique is used to detect the victim that they belong to that clone attack and the detection of cloned profile is done by the use of recording foreign IP [3].

Fake Profile Detection is an algorithm; techniques have been developed to identify the duplicate of the online presence to prevent the Sybil attack. This made a difference between the trusted and untrusted users.

Socware Detection is a technique which prevents the damage of the posts in the facebook this can be fully avoided by removing and detecting the malicious code.

Prevention and avoidance of the sensitive information. The certain implementation and prototype is used to detect and prevent the Location and Information leakage [15]. Preventing of the Location details will put an end to all kinds of the major threats.

CONCLUSION

Cyber bullying is dangerous with negative outcome to both bully and victim but it can be resolved using the proposed system. The proposed system is designed in such a way that it can mitigate the cyber bullying attack completely and to provide a trust worthy social networking service to the end users in a reliable manner. Further, the proposed system can be extended to prevent Online Predators which is creating lot of issues and risks to the social network users.

REFERENCES

[1] Accessed online social networking group, (Facebook), 8 June. [Online]. Available: http://www. facebook.com/ [8 June 2015]

[2] Accessed online social networking group, (Facebook), 18 September. [Online]. Available: http://nobullying.com/three-real-life-stories-of-cyber-bullying/ [18 September 2015]

[3] Accessed online social networking group, (Facebook), 28 September. [Online]. Available: http://www.scambusters.org / identitycloning.html/ [28 September 2015]

[4] Accessed online social networking group, (Facebook) , 28 September. [Online]. Available:http:// fox8.com/ 2015/03/ 26/two-teens-arrested-after-posting-video-on-facebook-of-them-damaging-a-police-car/ [28 September 2015]

[5] Accessed online social networking group, (Twitter), 14 June. [Online]. Available: http://www.twitter. com/ [14 June 2015]

[6] Accessed online social networking group, (Tumblr), 14 June. [Online]. Available: http://www.tumblr. com/ [14 June 2015]

[7] Accessed online Social networking group, (VKontakte), 21 June. [Online]. Available: http://www.vk. com/ [21 June 2015]

[8] Facebook, Facebook Reports Fourth Quarter and Full year 2015 Results, accessed July. 14, 2015. [Online]. Available: http://investor.fb.com/ releasedetail.cfm?ReleaseID=821954

[9] Feinberg, J 2015 Social networking group, 18 August. Available from: <http://www. wordle.net/> [18 August 2015]

[10] Google+, accessed June. 9, 2015. [Online]. Available: https://plus. google.com/

[12] Michael Fire, Member, IEEE, Roy Goldschmidt, and Yuval Elovici, Member, IEEE," Online Social Networks: Threats and Solutions", (2014) IEEE Communication Surveys & Tutorials, Vol.16 , No.4, Fourth quarter 2014, pp. 2019-2035. Available from: http://ieeexplore.ieee.org / stamp/ stamp.jsp? arnumber=6809839 /

[13] Pew, P 2015, *Social networking group, (*Social media statistice),1September.Availablefrom:<http://www.pewinternet.org/2015/01/09/social-media-update>. [1 September 2015]

[14] Pew, P 2015, *Social networking group, (*Social media statistice),30September.Availablefrom:<http://www.pewinternet.org/fact-sheets/social-networking-fact/>.[30 September 2015]

[15] Sina Weibo, accessed June. 14, 2015. [Online]. Available: http://www. weibo.com/

[16] Wikipedia, List of Virtual Communities With More Than 100 Million Active Users, accessed September. 8, 2015. [Online].Available:http://en.wikipedia.org/wiki/List_of_virtual_communities_with_more_than_ 100_million_active_users