DOI: http://dx.doi.org/10.26483/ijarcs.v9i1.5455

ISSN No. 0976-5697

Volume 9, No. 1, January-February 2018

International Journal of Advanced Research in Computer Science

SURVEY REPORT

Available Online at www.ijarcs.info

COMPARATIVE STUDY OF THREATS AND SOLUTIONS IN ONLINE SOCIAL NETWORKS

Sowmya P
Department of Computer Engineering
Pillai College of Engineering,
New Panvel, Maharashtra, India

Madhumita Chatterjee
Department of Computer Engineering,
Pillai College Engineering,
New Panvel, Maharashtra, India

***Abstract*:** The popularity of social networks is increasing day by day to such an extent that people have become addict to it. Large proportion of users are teenagers. But most of these users are not aware of various security and privacy risks affecting these social sites like identity theft, sexual harassment, spamming and many more. The OSN users readily share a lot of personal and private information in the network like phone numbers, email address, family relations, bank details, home address etc. This information can be easily hacked by hackers and attackers. There are lot of solutions available in the market to fight against these threats. So, a thorough review of various security threats affecting the OSN users are discussed along with examples. Also, some existing solutions to fight against these threats are also discussed.

Keywords—OSN, Online Social Networks, threats, solutions

1.INTRODUCTION

Online Social Network (OSN) can be referred as virtual community where people share photos, videos, chats, likes, comments or views to build social relations with others who have similar interests.

The first modern social network was launched in 1997 and it was named “Six Degrees”. It allowed people to create profiles and become friends with other people. The OSN users share a lot of details in the network like photos, videos, school name, college name, phone numbers, email address, home address, family relations, bank details, career details etc. This information if put into hands of attackers will lead to several losses.

Most of the OSN users do not know about various security threats that exist in these networks like phishing attacks, spamming, fake profiles, malwares, identity clone, online predators, cyberbullying etc. The risks are more dangerous if the users are children.

There are various commercial tools which are available that can be used against these attacks. The social network operators are also providing several authentication and privacy mechanisms to protect users against these threats. So, these solutions help to protect our intimacy and privacy in social networks.

II THREATS

As the usage of social networks are rising day by day, the threats related to privacy and security to the users of these networks are also increasing. Fig 1, shows how the threats can be classified under different classes.

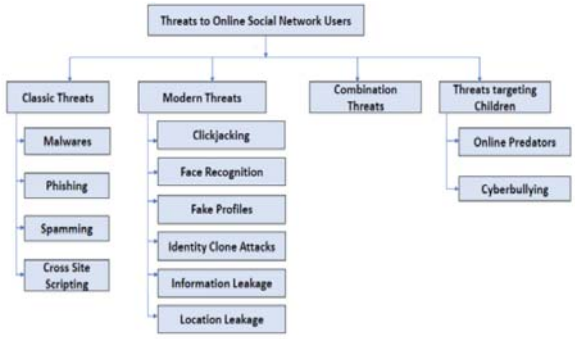

Fig 1: Classification of threats

A Classic Threats

Classic Threats make use of the information available in social networks to attack the victim and also his friends by adjusting threats to accommodate victim’s personal information.

The following are some of the classic threats which are affecting the OSN users

- ***Malwares*-** Malicious Software in short Malware is specifically designed to gain access or to damage the victim’s system without his knowledge. Koobface was a computer virus which gathered sensitive information like credit card numbers and personal information from Facebook and Myspace. Locky ransomware encrypts victims' files with RSA-2048 and AES-1024 algorithms and demands a ransom amount for the key, was installed into victim’s system through Facebook and LinkedIn security vulnerabilities.
- ***Phishing*-** In Phishing attacks, attackers use fake websites and emails to fool the victims to surrender their personal and private information. The victims will be directed to websites where they will be asked for information like password, credit card details, social

security number, bank details. One of the phishing attacks in 2017 was Google Docs Hack where nearly 3 million workers were forced to stop work when they got email invitations on Google docs to edit documents from attackers. When the recipients opened the invitations, they were redirected to third party app, where individuals' Gmail accounts were hacked.

- ***Spamming-*** Spamming uses electronic messages to send unwanted messages to users. It also includes sending messages repeatedly on the same site. Spammers in OSN, send advertisements to other users by using fake profiles. Trust in friends make the victims to read the spam messages and believe in the fake contents.
- ***Cross Site Scripting (XSS)-*** It is a code injection attack which allows the injection of malicious code into the website. Information like cookies, session IDs, passwords can be accessed by the attackers. One example is, Tweet deck XSS worm attack where the attacker spread malicious content to all Tweet deck users via Twitter. The result of this was compromise of mass Twitter accounts.

B Modern Threats

These threats are unique to OSN environment. They usually target users and their friends' personal information.

- ***Clickjacking Attack-*** Clickjacking is one in which an attacker tricks the user to click on something different from what he perceives to be clicking on, thus potentially exposing confidential data. Usually an invisible frame covers the content. When user clicks, it actually clicks on the invisible layer which start some other action. On Facebook, we have "Like-jacking" which emerged as a combination of Clickjacking and "Like" feature. A new type of attack is "Share-jacking" which is a combination of Clickjacking and "Share" feature [3].
- ***Face Recognition-*** Users use OSN to upload photos of themselves and their friends. These photos are publicly available to view and download. The attackers can use these photos to create biometric database, which will be used to identify OSN users without their knowledge. So, Face Recognition has become a very serious privacy issue in OSN. FindFace is a Face Recognition technology-based app developed by Russians which helps to photograph strangers in a crowd and help in finding their real identity by connecting them to their social network accounts. This put the public anonymity in risk.
- ***Information Leakage-*** In OSN, the users can share and exchange information among friends and other users. This information if mined by attackers can lead to Information Leakage Attack. The attack tries to disclose the user's unrelieved secrets.
- ***Location Leakage-*** Social media sites use location-based services to allow users to check in at their current locations which relieves the user's current location to all those who are connected to the network. The users expose their location information when they share photos and videos which are embedded with Geotagging information. This information can be used by attackers to track user's whereabouts. And this may also invite burglars and thieves to our home or business.
- ***Fake Profiles-*** The registration process in OSNs are very easy in order to attract more users. As a result, the process of creating fake profiles have also become easier. The attacker creates fake profile and try to connect to the victim. In most of the cases the attacker uses victim's opposite sex information in order to accept his friend request. By accepting the friend request, the victim will expose all his private and personal information to the attacker.
- ***Identity Clone Attacks-*** Profile Cloning is identity theft of existing user's credentials in order to create a duplicate profile using these credentials. There are two types of cloning namely same site cloning and cross site cloning. In same site cloning, the attacker uses the credentials of a user from one OSN to create cloned profile in the same OSN. In cross site cloning, the user credentials are taken from one OSN and duplicate profile is created in another OSN. The cross-site cloning is very difficult to detect [4].

C Combination Threats

Attackers can combine classic and modern threats in order to create a more severe attack. For example, an attacker can use a phishing attack to collect a targeted user's Facebook password and then post a message containing a clickjacking attack on the targeted user's timeline, thus luring the user's Facebook friends to click on the posted message and install a hidden virus onto their own computers [1].

D Threats Targeting Children

Children are active users of Internet and they have become addict to it. As a result of this they are exposed to large number of online threats.

- ***Online Predators-*** Online Predators are those who exploit children and teenagers for sexual or violent purposes through Internet. This include child grooming, online harassment, unwanted exposure of photos, engage in sexual activities, threats causing fear, mental torture etc. The reason for this attack is oversharing of personal information in social networks. The predators get all information about the victim like photo, phone number, address, date of birth etc. Also, sites like Facebook and Twitter even share the current location of the victim. When predators are getting all these information, their job is very easy. Online Predators mask their true identity to make the teens to meet them which have led to rape and even murder.
- ***Cyberbullying-*** In Cyberbullying, the attacker harasses his victim by sending hurtful messages, publishing embarrassing videos of the victim or by engaging in other inappropriate behaviors. Cyberbullying usually affects children, rather than adults [1] and they are often motivated by anger, revenge, depression or frustration. Sometimes they do it for entertainment. A significant amount of bullying takes places in sites like Facebook. This is due to its widespread popularity and its capacity to share photos and videos. Bullying can lead to feel angry,

alone, isolated, depressed and can even lead to suicide.

III SOLUTIONS

There are various solutions to fight against the threats in OSN, but most of the users are unaware of it. The solution can be classified as shown in Fig 2

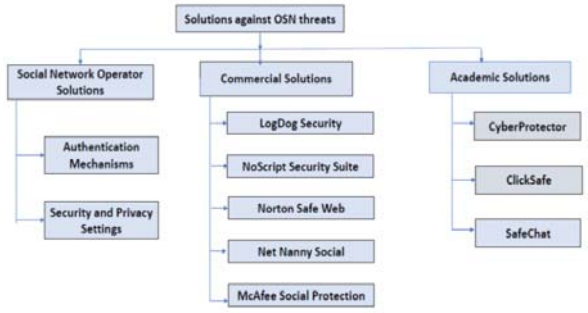

Fig 2: Classification of Solutions

A Social Network Operator Solutions

OSN operators attempt to protect their users by activating safety measures, such as employing user authentication mechanisms, applying user privacy settings, providing internal protection mechanisms and options like report users [1].

- ***Authentication Mechanism***- OSN operators use authentication mechanisms, such as CAPTCHA, photos-of-friend's identification and in some cases the user send a copy of his or her government issued ID [1]. Facebook uses two-factor authentication mechanism called "Login Approvals," which ask the user to not only insert a password but also provide a verification code that was sent to the user's mobile device when signing into the account from a new or unrecognized system. This prevents an attacker from logging in through hijacked accounts and using it for vulnerable purposes.

- ***Security and Privacy Settings***- Many OSNs support various configurable user privacy settings that enable users to protect their personal data from other users or applications [2]. Privacy settings exists in Google+ where users place each one of their friends into groups, also known as circles, such as Best Friends circle, Work circle, and High School Friends circle [2]. Using these circles, Google+ users can better protect their privacy by deliberately choosing which of their posts are exposed to each circle [2].

B Commercial Solutions

Various commercial companies, in spite of their traditional security options, have many software solutions to better protect the OSN users from threats.

- ***LogDog Security***- LogDog is a firewall-like android app which helps to protect user's private information. It takes on the role of a 24-hour-a-day watchdog. The application closely monitors online accounts, continuously scanning for various unauthorized-accesses. If a hacker attempts to gain access to any of the accounts, an alert that there is unauthorized access will be received, allowing to take back control of accounts as soon as possible. The app currently monitors Facebook, Gmail, Evernote, Yahoo and Dropbox accounts, but the company also plan to add more social platforms in future.

- ***NoScript Security Suite***- It is an open source extension to Mozilla base web browsers which allows executable web content such as JavaScript to run only from trusted domains of user's choice. It protects OSN users from Clickjacking and XSS attacks by blocking executable web content running from untrusted websites. Some websites are already added to whitelist by default, but user has access to add or remove items at any time. It also provides options to block objects, styles, images and media as well.

- ***Norton Safe Web***- It is an online service that allow the user to check whether a particular website is safe before viewing it. So, it ensures the user to search, surf and shop any website that are free from cyber threats. Norton Safe Web for Facebook is a program which scans Facebook user's news feeds and identifies any risky links, malicious downloads or unsafe sites. As all the scanning are done behind the scenes, user never know that it is running until he gets a message that something might be wrong.

- ***Net Nanny Social***- Parents are always worried about their child's online friends, photos, videos, posts and other social network interactions. Net Nanny is a cloud-based dashboard that helps parents to monitor the social networks where their kids have accounts. It monitors activities related to child's friends, cyberbullying, online predators, child pornography, privacy concerns etc. Parents can access their child's list of friends, to monitor activities related to those friends. There is an option to activate alert notifications. Once done, parents receive email or message when harmful or inappropriate activities are detected on their child's social network accounts.

- ***McAfee Social Protection***- It is a free application for Facebook that protects user's photos from being shared without his permission. User can select which of his friends can have access to his photos and can make the photos blur to everyone else. Photos are encrypted so they cannot be copied or printed and only the friends who the user invite to see are able to see them.

C Academic Solutions

Several recently published studies have proposed solutions to various OSN threats. These solutions provide cutting-edge insight into dealing with social network threats [1].

- ***CyberProtector*** - It is a proposed method used to find malicious links in the emails using lexical and host-based features in the URLs. It

uses Naïve Bayesian classifier to find whether URL is legitimate or not. It counts up the occurrence of each feature in an email and calculate the cumulative score. If the score is greater than given threshold, URL is malicious otherwise it is legitimate. The features considered are [5]

- URL Length longer than 55 characters
- HTTP Status not ok
- URL contains an IP address
- Number of dots more than 5
- Domain age not checked
- URL contains a phishing keyword

- ***SafeChat*** - SafeChat is a tool used to shield children's communication from explicit messages. It is the result of aggregating context-based authentication features and message encryption features. SafeChat filters explicit words without recognizing their meaning. Such an approach hardens the system against malicious attacks. Furthermore, it secures the communication channels against possible man-in-the-middle attacks by employing an encryption mechanism. In addition, [6] it encompasses the tools to authenticate and authorize communications and allows parents to monitor children communication channels in case an intervention is desirable. Fig 3 shows the SafeChat Architecture [6] where

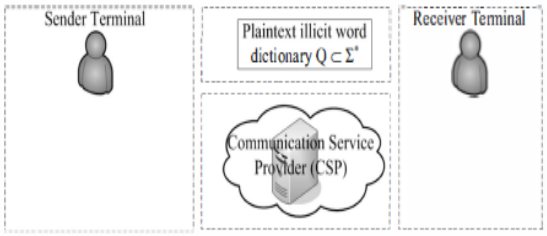

Fig 3: Architecture of SafeChat [6]

- Illicit Word Dictionary: SafeChat initially fetches offensive words set from WordNet followed by all the senses (synonyms) of them plus their declined or conjugated variants. Altogether, SafeChat prepares a dictionary of explicit language words [6].
- Terminal: Expose user friendly tools for users to communicate with other users in the framework, assumed each user is associated with a terminal [6].
- Communication Service Provider (CSP):[6] It is the backbone of the task to protect kids from receiving offensive messages. It is a regular messaging facility provider but employs an internal or external plug-in to digest offensive messages to block such messages from reaching kids.

- ***ClickSafe*** - ClickSafe is a browser-based tool used to provide increased security and reliability against clickjacking attacks [7]. ClickSafe is based on three major components namely Detection Unit, Mitigation Unit and Feedback Unit. Fig 4 shows the architecture of ClickSafe [7] where
  - Detection Unit: It is responsible for detecting clickjacking on a rendered webpage by searching for an element that is redirecting the user to an external page both implicitly via JavaScript as well as explicitly via HTML anchor tags [7].
  - Mitigation Unit: When an external link is clicked, the click is intercepted and a popup displaying both the URL the user clicked on, as well as the site's rating is presented to the user. The user then has the option to either continue with the action or cancel his redirect attempt [7].
  - Feedback Unit: It records the user's actions and converts them into ratings and allows future interactions to be more informed [7].

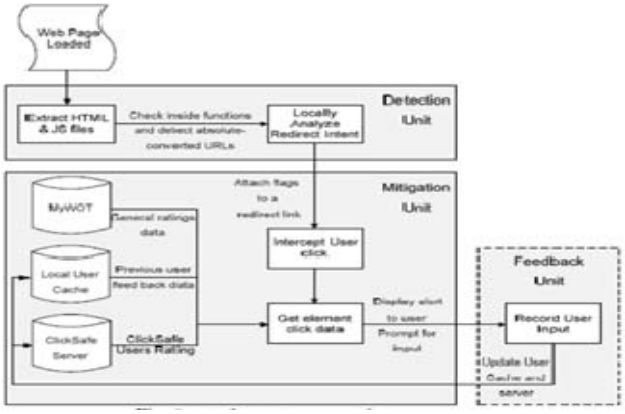

Fig 4: ClickSafe Architecture [7]

IV COMPARATIVE ANALYSIS

Table 1: Comparative Analysis of Threats and Solutions

Threats / Solutions	Malware	Phishing	Spamming	XSS Attack	Clickjacking	Face Recognition	Fake Profiles	Identity Clone	Information Leakage	Location Leakage	Online Predation	Cyberbullying
Authentication Mechanisms		✓	✓				✓	✓			✓	
Security & Privacy Settings			✓			✓	✓		✓	✓	✓	✓
LogDog Security	✓	✓	✓									
NoScript Security Suite		✓	✓	✓	✓							
Norton Safe Web	✓	✓	✓	✓	✓							
McAfee Social Protection						✓			✓	✓		
Net Nanny Social							✓				✓	✓
CyberProtector	✓	✓	✓									
ClickSafe	✓	✓	✓	✓	✓							
SafeChat							✓				✓	✓

The comparative table shows various threats which we studied and the solutions that can be used against these threats. No solutions will provide full protection to a user's privacy and security. In order to be well protected against

the threats, users must be careful about what information they post.

V CONCLUSION

It can be concluded that no solution provides complete protection to user's privacy and security. We should be very much careful in what we share and post as the OSN is a vast environment where there are millions of users including attackers and hackers. Parents should frequently monitor their children's activities in OSN. Once the user gets to know about various threats in OSN and solutions to protect themselves from these attacks, then Online Social Networks will become a wonderful experience for every user.

REFERENCES

[1] Michael Fire, Member, IEEE, Roy Goldschmidt, and Yuval Elovici, Member, "Online Social Networks: Threats and Solutions", JOURNAL OF LATEX CLASS FILES, VOL. 11, NO. 4, IEEE Communications Surveys & Tutorials, DECEMBER 2012, DOI 10.1109/COMST.2014.2321628

[2] Yong Wang and Raj Kumar Nepali, "Privacy Threat Modeling Framework for Online Social Networks", International Conference on Collaboration Technologies and Systems (CTS), IEEE, 2015, pp 358 – 363, DOI: 10.1109/CTS.2015.7210449

[3] Rakesh Singh Kunwar and Dr. Priyanka Sharma, "Social Media: A New Vector for Cyber Attack", International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), IEEE,2016, pp1-5, DOI:10.1109/ICACCA.2016. 7578896

[4] Georgios Kontaxis, Iasonas Polakis, Sotiris Ioannidis and Evangelos P. Markatos, "Detecting Social Network Profile Cloning", International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), IEEE, 2011, pp 295-300, DOI:10.1109/PERCOMW.2011.5766886

[5] Nureni Ayofe Azeez and Ademolu Oluwatosin, "CyberProtector: Identifying Compromised URLs in Electronic Mails with Bayesian Classification", International Conference on Computational Science and Computational Intelligence (CSCI), IEEE, 2016, pp 959-965, DOI: 10.1109/CSCI.2016.0184

[6] Gunter Fahrnberger, Deveeshree Nayakt, Venkata Swamy Martha and Srini Ramaswamy, "SafeChat: A tool to shield Children's communication from explicit messages", 14th International Conference on Innovations for Community Services (I4CS), IEEE, 2014, pp 80-86, DOI: 10.1109/I4CS.2014.6860557

[7] Jawwad A. Shamsi, Sufian Hameed, Waleed Rahman, "Clicksafe: Providing Security against Clickjacking attacks", 15th International Symposium on High-Assurance Systems Engineering, IEEE, 2014, pp 206-210, DOI: 10.1109/HASE.2014.36