Security and Privacy in Social Networks

Pranathi Alla and Sandhya Bairi

Abstract Social networking sites such as Facebook, Twitter, Friendster, Tribe have gained thriving popularity in recent years due to internets wide adoption. These services offer millions of individuals the basic features of interaction, communication by letting them create online profiles and share personal information with expansive network of friends and even strangers. While revolutionizing the way users interact with their friends, they have also become a potential means for an adversary to exploit and cause significant harm to users, due to its large user base and and huge amount of information. Social networking sites try to prevent such misuse, but many attackers are still able to surpass those security measures by using various techniques. This paper presents different security and privacy issues in social networks and certain ways of dealing with such issues.

1 Introduction

Social Network Services (SNS) are presently transforming the way people interact and communicate with one another. Such services are offered online and centralized by Online Service Providers (OSN). Preservation and authorization to these OSNs are handled by Social Network Providers (SNP). Huge amount of Personally identified information given by the users is stored in databases under the maintenance of SNPs. Social Networks are web applications that usually follow client-server architecture. They are approximated by social graphic models connecting several individuals or organizations. These networks allow users to create profiles in which users share their information which can be kept public as well as private based on users interests and build relationships with other users of mutual interests resulting in an online community. People invest a lot of time on social networks every day spreading their community. The information that users share or post can be geographic, contact, images, videos etc. While social networks have been very helpful in expanding friend networks, they have also been attracting certain adversaries who

try to take advantage of certain delicate information being posted or which is already available for malicious or commercial purposes.

2 Related Work

In [1], an information leakage method is described which quantifies the amount of information available about a user. It explains ways to protect users privacy and reduce information leakage in the social Web. The authors also highlight the importance of effective countermeasures for personal information leakage. Geo-social networks (GeoSNs) in [2], extend social networks in which geographic services like geocoding are used to provide additional social dynamics. It facilitates user coordination and interest matching by associating location with corresponding users and content. The location can be either user submitted or derived from geolocation techniques. Four privacy aspects related to location, co-location, absence and identity privacy in GeoSNs, are explained addressing potential attacks and protection techniques.

Mobile social networks make substantial use of user location. Privacy Context Obfuscation (PCO) is a method that masks the location information with respect to parameters like the time of day, people who can access location data etc. [7] This is rather robust way for the users to secure their information by classifying the strangers to not be able to view their data. Theres another method for sharing location information which is more robust than PCO, described by Wei, Xu and Li in [8] for preserving privacy in Mobishare. This technique includes the online social network provider with identities and third party location server with locations and there is no mapping between these two. Hence the online social network provider can never know the location information and the location server does not know the identities of the location information it handles.

[3] examines the friend-in-the-middle attacks on social networks that mimic social network applications. It also depicts various ways adopted by the attackers to automatically gather social data. The adversaries can use this data for large-scale attacks involving social phishing and context-aware spam. Apparently, all prime social networking sites are susceptible to this kind of attack reason being failure to properly protect the network layer. With reference to the disclosure and protection of privacy of relation over online social network information, [4] addresses certain challenges. Existing techniques to secure privacy of the relation is classified based on the maximum revelation of the user identities.

The online social network provider is able to see all data that flows through the network. The present privacy policies and terms of usage agreements signed by the users are in favor of the provider. Users no more want to trust OSN providers with their personal information. Anderson et al. in [4] designs a social network in the client/server architecture that does not depend on the OSN provider. The server only provides availability i.e. name resolution of members in the social network. The actual content is present on computers of the individuals spread across the Internet.

Any message that is meant for an offline user stays locally until the receiver comes online the next time. Therefore actual message never passes through the server not stored on it at any time. However, this does not have an advantageous revenue and hence not followed.

The best way to keep data private is to use encryption. One such system flybynight is explained in [5] wherein a Facebook application that enables users to send encrypted messages to each other. A public/private key pair, which is encrypted with a user provided password is created when a person first uses the application. When one user wants to send a message to a friend, message is entered in flybynight web form which encrypts it using client side javascript and links it with friends id and is transmitted accordingly. However since the random number generator of javascript is not enough for encryption, this has issues. In [6], Luo et al. suggests another system called facecloak". This is a Firefox browser extension that has three phases namely setup, encryption and decryption. In the setup phase, three keys are generated, of which master key is involved in encrypting the message being posted as well as in decryption. Access key is retained for the local purpose of the user. However, this still has the trust problem.

With reference to a basic implementation of distributed online social network in [12], data is stored locally in an encrypted format. When a new piece of data is generated by the user, it is public or private encrypted and the user specifies who can access this data. The users who are allowed access are provided with the public encryption key. The keys are split in such a way that the user who posts it, has fifty percent and the authorized users have the remaining 50 percent. In fact, only fifty percent is required by anyone to decrypt the actual data. The authorized users can get it from the user directly or from the others in the authorized group. The data storage is simple in nature since the data is stored locally. Its usability is based on dedicated server that every user must run. Its robustness is limited to one node failure only. However, distributed online social networks also suffer from several technical security and privacy challenges.

Abbas et al. in [14] addresses the node availability problem by designing a system that supports links of low reliability using simple gossip protocol. An unanswered friend request is tried every five minutes for one day and then once every 24 hours for one week. But this doesnt take into consideration security or privacy of such network. Backes et al. develops an API framework in [13]. They present a framework with extensive use of cryptography to achieve access control, secrecy of resources, privacy of social relations, and users anonymity in social networks. The main idea is that any DSN system can be designed using API calls so that more focus can be put on issues like distributed content sharing, friendship in case of node failure. The cryptographic protocols that are used to apply these calls use pseudonyms to initiate social relations thus, guaranteeing the anonymity of users. This method does not put any limitation on the underlying social network and hence is applicable for decentralized social networks.

A robust system OneSwarm" that addresses privacy in a distributed social network directly is designed in [10]. It offers privacy in peer to peer data sharing applications like bittorrent. For instance bittorrent is not totally anonymous since the

users connect to each other via IP addresses which can be detected. As of now, solution for this problem is to use proxy services to hide ones IP address. But this leads to performance overhead as the packets are required to be routed to random hosts through the proxy. OneSwarm provides a solution that is beneficial than proxies. The basic perspective of this system is to apply the proxy only when searching for content and only internally through other users of the network. One can find content anonymously this way and the content supplier can also find out if the person has proper authorization to access the files. Then the peers can connect by looking for those who have the required content without giving up their own IP address. The standard technique for performing network analysis securing privacy is Anonymization which requires the presence of a trusted third party, who is totally familiar with complete network. [9] proposes an another method wherein the desired analysis can be performed by the decentralized parties who maintain the network in such a way that no third party would be necessary and the topology of the underlying network is not exposed. Multi party protocols for secure social network analysis are designed along with a proper implementation of usual network analysis measures such as closeness centrality and PageRank algorithm.

Since in DSNs user profiles are stored on the peers of the users belonging to the network, one of the main issues is related with the availability of the profile when the data owner is not online. [11] proposes a DSN which depends on a friend-to-friend peer to peer overlay where the users data is stored only on friend peers. This follows the ego-network concept, which considers the social network from the local viewpoint of a single user. A distributed algorithm based on the extent of the ego-network is proposed which makes sure that users store their data only on the peers of their friends. In this way any online user can extract the private data of its offline friends through a common online friend.

3 Overview

The functionality of online social networks can be classified into three kinds. The networking functions update the user profiles once created, that is the vertices and edges of the social graph depicting actors and connections respectively. The data functions manages the user provided information leading to a better interaction among the users. The access control functions manage the authorized access to the content provided by the user.

SNS services are usually divided into three layers based on their functionalities. Social Network layer represents the users and their connections. Application Service level represents the architecture and organization of the management. Communication and Transport Layer takes care of the actual communication that takes place through the network.

Cybercriminals follow two methods to exploit user information namely social engineering and reverse social engineering (RSE). Both have a common goal to misuse social network content although both follow different approaches to do so.

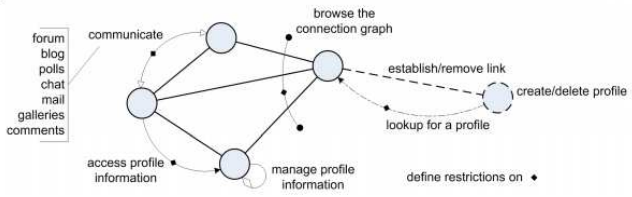


Fig. 1 Main functionality of a typical OSN architecture

Social engineering involves attackers actually approach the existing users in order to launch a successful attack whereas RSE involves indirect approach of misdirecting the users into bad influence to make them commit faulty errors leading to the compromise of their information. These methods were used before spamming, malware etc. came into picture. Different methods of implementing reverse social engineering are leveraging the friend recommendation feature of the network to acquaint the adversaries with the users, exploiting users location information, mutual interests or common search history.

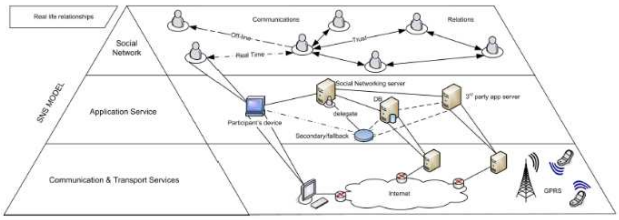


Fig. 2 Architectural layers of social networking services

Some of the privacy and security issues that social networks faced today can be classified into the following. They are privacy issues, identity theft issues, spam issues, malware issues, and physical threats issues.

3.1 Privacy issues

The security of communication gives rise to the need for certain inference techniques that are concerned with interpreting any kind of data with respect to: (1) Anonymity - this means that without disclosing identities any relevant resources or services should be gathered. (2) Unobservability - the requirement that no outsider ought to accumulate any data about the communicating parties and the substance of their correspondence (3) Unlinkability - this is the requirement that when two messages have been received, no third party must be able to determine whether both

messages were sent by the same sender, or to the same receiver; (4) Untraceability-this is the demand that no third party can build a history of actions performed by arbitrary users within the system;to word it differently, it demands both anonymity and unlinkability.

By profiling we understand an attack against any target OSN user aiming to collect information about OSN activities or further attributes of that user. The attack is usually performed by OSN users, possibly in an automated way, since the collectable information is publicly available by all OSN users. The profiling attacks performed by OSN users has certain risks that can be diminished via fine-grained access control and anonymizing techniques. For example, clients ought to have the capacity to enable access to the individual parts of their profile on the singular, individual basis and not only based on roles (e.g. friends) as realized in many current OSN platforms. However, the recent studies, show that even if the personal information is hidden, the data can be gleaned from public information and social activities of the user. An alternative approach to tackle this problem could be to let users decide whether the profile activities (e.g.discussion comments) should be not be linked to their profiles.Admittedly these measures might reduce the risk involved, baulking profiling that is performed by OSN providers now appears to be much harder.

Through secondary information accumulation it can be understood that an attack that aims to collect information about the owner of some OSN profile via secondary sources apart of the OSN platform. Generally an example of such data collection is when a search engine is used discover data that can be connected to the profile proprietor. More successful technique is to utilize a particular Internet service that totals all data it can discover about some specific individual. With the usage of such an attack the adversary can glean plenty of information about some user than available in the profile and misuse it against the user both in the virtual environment of the OSN platform and in the real life. Another example are recent de-anonymization attacks is that misused the group memberships of social network users for their unique identification. Besides, the presence of OSNs with public and private profiles rearranges the auxiliary information accumulation the same number of clients have a tendency to have accounts on various stages. There is no significant insurance against secondary information accumulation assaults since the information is regularly totaled from various areas. In this manner, it is the obligation of the client to constrain data kept in the profile so as to keep away from its linkability with optional sources.

In numerous social networking sites, clients utilize their genuine name to represent their records. Thus, their profile is presented freely to other interpersonal organization clients, and also every other person in the online world. In social networks the user profiles are indexed by search engine and the top rank results usually entail them. In the situation discussed, if attackers know the name of the victims, they can easily search for victims profile, or they can search through social networking sites to obtain new victims. Aside from the basic utilization of genuine name as record name, there are additionally different techniques that can be utilized to uncover social network users anonymity. The two methods that shall be discussed are de-anonymize attack and neighborhood attack.

3.1.1 De-Anonymization Attack

In the above mentioned attack the area assault is expanded with nearby node data. They accept the attacker had information regarding two sorts of data. First, the local (node-based) features such as degree of a node, and, second, neighborhood (ego-based) data such as which nodes a node is connected to and which nodes those nodes are connected to. The system gives third type of data as outputs and are understood as regional features which is said to exposes behavioral. This data can intuitively be understood as the connection between nodes. This is at its essence different from the node label and in certain scenarios the more useful information. The sole purpose of labels and the reason for their value is because it is presumed the label can connect the entity to even more information. In reality, recognizable proof is the demonstration of associating data. This method relies on social impact or homophily and it is complex and theoretical.

Gilbert Wondracek, and his team have shown that by using group membership information and history stealing technique, the anonymity of attackers could be revealed in social network users. In the mentioned methodology, the attackers must understand that in which social network group (group of users that shares similar interests) victims belong to. The social network group is the one being focused on since the number of a social network individual user is much larger that the number of groups in social networks. Therefore, it is relatively easier to first focus on the group, and then use said group to gain access to any particular user. Attackers will steal history as a method to gather information on the URLs that the victims visited in their history to find out victims group.

	Security Objectives		
	Privacy	Integrity	Availability
Attacks			
Plain Impersonation	x	x	
Profile Cloning	x	x	
Profile Hijacking	x	x	
Profile Porting	x	x	
Id Theft	x	x	x
Profiling	x		
Secondary Data Collection	x		
Fake Requests	x		
Crawling and Harvesting	x		
Image Retrieval and Analysis	x		
Communication Tracking	x		
Fake Profiles and Sybil Attacks		x	
Group Metamorphosis		x	
Ballot Stuffing and Defamation		x	
Censorship		x	x
Collusion Attacks	x	x	x

Fig. 3 Attacks Vs Security objectives in online social networks

In social networking sites there are two different links. A static link which is uniform for all network users.ad is used in showing the home section to the user as

well as a dynamic link which holds that pertains to an individual user data in the group.

When attackers want to steal history they attract the users to their websites and and they try to gain access to users browsing history by sending out a list of URLs. This is the URL of social network group that users could be a part. The mentioned links can be easily gathered via group directory which is provided by the help of social networking sites. Then the attackers check whether the URLs are visited by the victim by looking through their history. This browsing history is again given back to the attackers. This gathering of mentioned history is done using conditional logic in CSS (Cascading Style Sheet). Therefore, by stealing history, victims browsing history can be gathered by the attacker, and then can be used to narrow down the links or URLs pertaining to an individual user. Usually, numerous social network groups give the group members mailing list. The obtained emails can be use by the attacker to identify user.

3.1.2 Neighborhood Attack

In this type of attack the opponent has an anonymized copy of the social network. This copy is a graph with edges and vertices but does not contain labels on vertices. The opponent also is aware of the graph information in the locality of the person trying to be identified in the graph. For instance they may know the individual being referred to has three neighbors (vertices associated straightforwardly by one edge) and that two of those neighbors are they, themselves neighbors. It isn't difficult to envision a graph where the profile of this individual may be self-evident.

Social networks can be spoken to by social graph where a node speaks to an Social network client, and an edge speaks to connection between two social network clients. Neighborhood attack depends on the idea that if assailants know the neighbors of the victims node, and the connection between them, at that point aggressors can recognize victims node. For instance, if an assailant realizes that A has five companions, two of A's companions (B, C) are companions with each other and the others three (D,E,F) are not companions, Figure 1 speaks to 1-neighborhood diagram of A. Attackers can utilize this diagram to distinguish A since 1-neighborhood graph is exceptional to every Social network node.

3.1.3 Users Profile and Personal Information

And in addition user's account , social network user's profiles for the most part contain genuine data about users. Delicate data, for example, user's full name, contact data, relationship status, date of birth, past and current work and education pulls in attackers. Thusly, the primary issue of user's profile is the leakage of profile and individual data. Sources of user's profile Leakage are:

1. Leakage of data through poor privacy settings: Most social network users are not watchful about their security settings. Many open their profile to people in

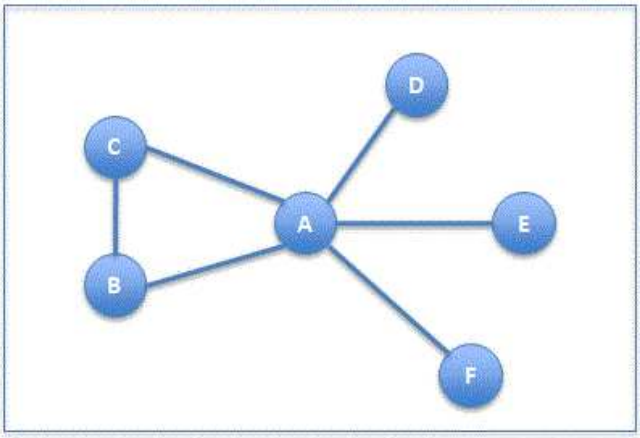


Fig. 4 Neighborhood graph of A

general so anybody can access and see their data. Additionally, numerous social networks default security setting is as yet not protected, for example, in Facebook, a companion of a companion who the user does not know can in any case observe his data. Nonetheless, even the most secure protection setting, there are still defects that enable attackers to get to user's data.

2. Leakage of data to 3 rd party application: Many social networking sites, for example, Facebook give an API (Application Programming Interface) for outsider engineers to make applications that can keep running on its platform. These outsider applications are extremely prevalent among social network users. When users include and permit 3 rd party applications to get to their data, these applications can get to user's information consequently. It is additionally fit for posting on user's space or user's friend's space, or may get to other user's data without user's learning
3. Leakage of data to 3 rd party area: Many lsocial networking sites utilizes 3rd party domain service to track social network users activities, or permits advertisement accomplice to access and total social network user's information for their business advantage.

3.2 Identity Theft issues

Identity theft is a method of taking somebody elses identity or personally identifiable information and using it a disguise for getting malicious things done. Since social networks are fantastic collection of such sensitive data, they lure attackers to commit these actions. There are several ways of stealing identities. One such way is by creating fake profiles called as plain impersonation. Sending confirmation mails does not prevent this since the adversaries will already be creating fake mail-ids as

well. This occurs majorly due to the fraud who try to involve in a convincing conversation thus gaining the victims trust. Such issues can be avoided by implementing more standard authorization techniques.

3.2.1 Profile Cloning

The motive of attacker here can be fulfilled in two ways namely existing profile cloning and cross-site profile cloning. This process involves creation of profiles that already exist either in the same social network which refers to existing profile cloning and if the profile already exists in another social network sites, it refers to cross-site profile cloning. Cross-site profile cloning is also known as profile porting since profile from one site is ported to create similar profile in another social networking site. In this method, the newly created profile will have almost the same content as the original one thus, appears similar thus creating a false identity. Even if the original profile is associated with some email since they will be kept hidden by most users, it wont make a difference. Thus confusion is created in distinguishing the original from the cloned profile. This may be followed by gaining access to private information from the friends of the original profile owners community. This process can be automated using tools such as iCloner which can collect the data, find matches and also send friend requests as well. In order to prevent such issues, standard techniques to identify the similarities between multiple profiles need to be deployed, one such mechanism being the cloned profile having later registration data compared to the original profiles. Profile porting is difficult to prevent because it requires cooperation between different social network service providers who are too cautious to allow access to one another to their secure divisions and departments.

3.2.2 Social Phishing

Phishing attack is performed as a result of profile hijacking. During profile hijacking, attacker wants to gain control over an existing profile. Since they are usually password-protected, attacker tries to crack the passwords using a dictionary attack provided it is a weaker one. Tools like iCloner also have automated CAPTCHA escape system thus rendering it useless. Other methods to get the password is by Phishing attack. In this kind of attack, adversaries facilitate a fake website that attracts the victims into giving their personal information such as financial or important identity numbers, passwords to the website. This depends on a fact that users will mostly use same passwords for different websites.

3.2.3 Crawling and Fake Requests

This process involves gathering lot of information that is openly available from several profiles and applications automatically. This is not similar to profiling where

particular users are aimed, also not similar to secondary data collection wherein sources other than social networks are leveraged. For crawling, the initial step is to send fake requests to the users who generally are more inclined towards spreading their online community and accept the requests no matter who it is. Thus it simplifies attackers access to user profiles and other personal information. The circulation of such attack is automated which is then used for crawling. This cannot be avoided because the main motive of social networks is to connect with each other and make new friends. The information thus collected from crawling is misused in many ways one of them being, selling it to various marketing agencies.

3.3 Spam Issues

Conventional spam attacks on email are now inefficient since usually such mail addresses are generated randomly or by crawling several websites. Techniques have been adopted by social networks wherein most of the spam stuff is being recognized and separated which the users delete within no time.

Spam attacks on social networks have become prevalent since security walls of social networks are not as good as mailing services. Spam may be in the form of news feed, posts and messages in social networks. Since people spend a lot of time on social networks, this is an added advantage to the adversaries. There may be inappropriate or irrelevant advertisements, links that can lead to automatic download of various kinds of malware without the users notice. This comes from the fake profiles wherein adversaries create profiles pretending to be either a famous person or friend or follower of the user to make friends and thus spread the spam to others as well. Using specific tools, once access has been granted to the application by the users, it will spam like a post or message and gets to friends timeline as well.

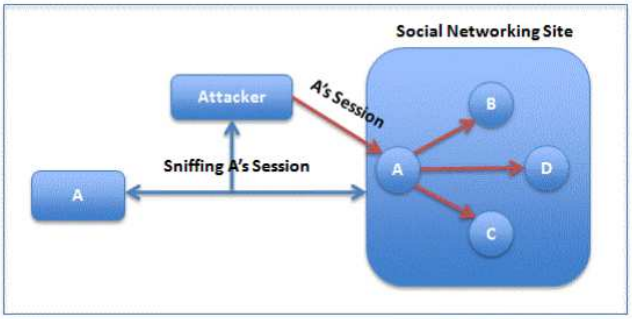
Since email is one of the best communication methods, it becomes the point of attack for adversaries. Most of the emails that people get today are spam. Since the traditional method of randomly generating list of email addresses by using combinations of names or by crawling internet will not be sufficient and effective, adversaries turned to social networks for accomplishing their tasks. Although email addresses are kept private in social networking sites, adversaries can still procure them by users first, middle, last names, date of birth etc. This can also be achieved though finding friend feature wherein people with mutual interests can be met online mentioning their email addresses. Adversaries can leverage this feature by using randomly generated email addresses to extract valid ones.

Two major types of spam are Broadcast Spam wherein adversaries broadcast emails to all email addresses in their lists. The contents on the email are not specific to any victims. Thus users can realise that they are spam, and easily remove them. The other is Context-aware Spam wherein adversaries collect context information from a users shared information such as news feed, date of birth, wall post, or relationship to social networks friends to generate email spam that matches users preferences. By using this method, the email click through rate greatly increases.

Security analysts advised people to remove their mobile phone numbers and addresses from the site, in order to avoid their contact details getting into the hands of rogue apps which spam individuals and encourage them to purchase false goods.

3.3.1 HTTP Session Hijacking

HTTP Session hijacking on social networking sites is a man-in-the-center attack that can be utilized to acquire setting data from victims, and also victim's friend's data that will later be utilized to produce context-aware spam. Figure 2 shows how session hijacking deals with social network users. To start with attackers endeavor to sniff communication between victims (A) and social networking sites, particularly those without information encryption. Diverse network attacks can be utilized as a part of this case, for instance, ARP cache poisoning or DNS poisoning. Attackers at that point catch HTTP headers that contain session cookies since numerous sites utilize cookie based confirmation. After that attackers would now be able to duplicate the HTTP session and utilize it to get to the casualty's profile and individual data. Moreover, aggressors can utilize the victim's profile to recover the victim's friend's (B, C, D) data, for example, email locations, and after that utilization of this data to create context aware spam.



3.3.2 Sybil attacks

In numerous OSN platforms user can without much of a stretch make a few profiles with conceivably unique characters and matter with profile. Since numerous OSN platforms absence of legitimate confirmation such production of phony profiles turns out to be simple. On the technical side, the client has just to make another email for the enrollment of a phony record. Counterfeit profiles pave the way for Sybil attacks that may fill distinctive needs. For instance, proprietors of phony profiles can set up new associations without unveiling their genuine personalities. Along these lines they may get more data about some individual than by utilizing

some genuine record. Sybil account may be made for the benefit of the entire group. Besides, Sybil records can be abused against the functionality of the OSN platforms. This incorporates circulation of spam messages or other unlawful substance, for example, malware and phishing links, illicit commercial, and so on. Formation of phony profiles can be viewed as an unique type of impersonation assaults. One answer for OSN suppliers to perceive counterfeit profiles is to utilize IP traceback. Without a doubt, if logins to a few profiles originate from a similar IP address then it is likely that some of these profiles are phony. Be that as it may, an assailant may endeavor to stay away from IP traceback by utilizing different proxies. Along these lines, more grounded recognizable proof and authentication mechanisms for affirmation of new users would offer a superior security.

3.4 Malware Issues

Since the fundamental idea of social networks depends upon relationship among users inside the systems, malware can without much of a stretch spread through this interconnection. Additionally, numerous social networking sites are as yet missing of the techniques to decide if URLs or embedded links are malicious or not. Consequently, attackers can misuse this imperfection. Malicious link can divert casualties to malicious sites, and afterward send noxious code to victim's PC to take data, or to utilize victim's PC to attack others.

1. Social Network API: The source of social network users information leakage can be 3rd party applications as mentioned. For this situation, these applications are additionally viable sources of malware infection as all the users have access to the application. In user's view these applications may look genuine, and appear to work as though it ought to be, yet inside it may shroud a pernicious connection that takes users to malicious space, and spreads malware to users.
2. Drive-by Download Attack: This kind of attack utilizes advertisement as a medium to spread malware crosswise over social networks. It is otherwise called malvertising attack. Attackers post malevolent ad on social network user's wall or message board. At the point when users click on advertisements, they will be diverted to the noxious sites that at that point will incite victims to download pernicious code, for example, Java or ActiveX substance to their program. At that point, their PCs will get contaminated with malware Recently, Facebook was looked with drive-by-download attack. This attack misuses malicious commercial that makes chain of infection. The Antivirus Company, Trend Micro found that "the promotions suppliers were associated with a specific Facebook application"
3. Cross-Site Scripting Attack: Cross-website scripting (XSS) is one of the web application vulnerabilities that keep running on a web program. Cross-site scripting bolsters JavaScript to victim's program. An attacker can compose dynamic HTML code to influence the web program to send victimcookies to attacker's server [Acunetix]. XSS Worm is an infection that spread itself consequently

among users who get to a malicious sites. It utilizes web program to spread malware to different users and take user's data. Since social networks depend on the network among clients, it is a decent platform for a XSS worm to spread out. The procedure of infection is that attackers will choose source node, which is a social networking users that will begin the spreading of the malware. Once the source node sign in to the social networking site, malware will take control of the program and command it to play out a few assignments. For instance, aggressors can go about as record proprietor by presenting or sending message on other informal community clients, add applications to the users record, or take the contact list. The source node will then spread malware to other social networking users who associate with it. The infection will spread as a fasten from one node to alternate nodes.

4. Clickjacking : Clickjacking is a method which attackers trap victims into tapping on a button or an item. At that point, the concealed code will be activated to play out some pernicious activity. For instance, Facebook likejacking, for this situation social network users will be given a video player that appears to be like YouTube video. While tapping on the video, rather than the video playing, the Facebook like button of the content is being activated. Subsequently, clients are deceived to like the page so the page can turn out to be more well known. What's more, some of these phony recordings may incite users to include some individual data previously seeing the video, so attackers can additionally get victim's data

3.4.1 Malware Examples

1. Koobface: Koobface is a computer worm that spreads across social networking websites such as Facebook and mySpace. This kind of worm unlike most spams which actually spread because most users deliberately share them, first affects the individual computer. Then generates itself onto the social networking sites.Eventually, it gathers victims login information to various websites or gains access to any sensitive financial information. It also uses the affected computers to build a bot-network that works in a peer-to-peer method. They receive orders to download different other malware with payment and spread their network by spreading fake messages. In fact, the first Koobface attack started with facebook wherein the users were asked to click on a link to update their adobe flash player for watching a video. The moment the installation is done, their PC gets infected and gets exploited.
   There have been recent events that account for several attacks on social networking sites like Twitter and Myspace. One such attacks on Twitter is Mikeyy worm which initiates by spreading links to open rival networking sites here, StalkDaily. If users click on that link, it automatically sends similar messages with links to other followers mostly resulting in all opening the links leading to success of the attack. This is similar to Samy worm that attacked MySpace in 2007. In order to

avoid such attacks, users should not click random links and are recommended to use trusted third party clients. Firefox browser has an add-on no-script that will not allow undesired scripts to run.
Another attack faced by twitter and twitter users includes transmission of shortened URL goo.gl that sends out tweets automatically. Attacks by shortened URLs are not new and are not tough to technically curb them. There are arguments which say that URL shortening methods are not totally harmful in regard to the word limit for a twitter post. Blocking the domain completely is not a good choice whatsoever. Tools like Tweetdeck allows users to know the full length link before proceeding to the URL.

2. Profile Spy worm: The spreading of the worm is done by tweeting a link for downloading a 3rd party application called Profile Spy (an application that is fake and promises to show the owners information regarding who has viewed their profile).With the end goal to download the application, certain personal information regarding the user must be filled this lets the attacker to obtain users information. Once victims account is infected, it will keep tweeting malicious messages to their followers.
3. Goo.gl worm: The mentioned attack makes use of a abridged Google URL to swindle users into clicking the link. The counterfeit link will redirect users to a non-original anti-virus website. A pop up in the website will display a warning that says users computer has become infected, and encourages users to download their counterfeit anti-virus software which in reality is a piece of malicious code.
4. Ransomware: Ransomware is a type of malicious attack which blocks access to a computer system until certain amount of money is paid. It uses personal information from social networks to send mails which appear to be legitimate but are in reality, fake. Cybercriminals leverage this method to deceive people into opening the email attachments thus leading to downloading the ransomware onto their computer. Immediately the ransomware locks intended files and then demands the person to pay hundreds of dollars in the form of digital currency bitcoin in order to unlock those files.

4 Conclusion

Security and Privacy are crucial topics in computer science. They are more important in case of social networks because it involves sensitive data which is Personally Identifiable Information thus making them more vulnerable to outside harm. Though social networking sites try to make use of several security mechanisms to avoid such issues, adversaries keep finding new techniques to interfere leading to huge damage. Social Network Providers need to secure their social networks. Instead of restricting user access, new techniques can be developed by putting effort in research and development both in academia and industry. Awareness should be created among users with respect to several attacks and ways to deal with such threats, care to be taken in choosing social relations and sharing personal information.

References

1. Danesh Irani, Steve Webb, Calton Pu, and Kang Li, 2011, *Modeling Unintended Personal-Information Leakage from Multiple Online Social Networks*
2. Carmen Ruiz Vicente, Dario Freni, Claudio Bettini, and Christian S. Jensen. *Location-Related Privacy in Geo-Social Networks*
3. Markus Huber, Martin Mulazzani, Gerhard Kitzler, Sigrun Goluch, and Edgar Weippl. *Friend-in-the-Middle Attacks: Exploiting Social Networking Sites for Spam*
4. Na Li, Nan Zhang, and Sajal K. Das. *Preserving Relation Privacy in Online Social Network Data*
5. Matthew M. Lucas and Nikita Borisov. *Flybynight: mitigating the privacy risks of social networking.*
6. Wanying Luo, Qi Xie, and U. Hengartner. *Facecloak: An architecture for user privacy on social networking sites.*
7. F. Rahman, M.E. Hoque, F.A. Kawsar, and S.I. Ahamed. *Preserve your privacy with pco: A privacy sensitive architecture for context obfuscation for pervasive e-community based applications.*
8. Wei Wei, Fengyuan Xu, and Qun Li. *Mobishare:Flexible privacy-preserving location sharing in mobile online social networks.*
9. Varsha Bhat Kukkala, Jaspal Singh Saini, and S.R.S. Iyengar. *Privacy Preserving Network Analysis of Distributed Social Networks*
10. Tomas Isdal, Michael Piatek, Arvind Krishnamurthy, and Thomas Anderson. *Privacy-preserving p2p data sharing with oneswarm*
11. Andrea De Salve, Barbara Guidi, Paolo Mori, Laura Ricci. *Distributed coverage of Ego Networks in F2F Online Social Networks*
12. Angela Bonifati, Hui (Wendy) Wang, and Ruilin Liu. *Spac: a distributed, peer-to-peer, secure and privacy-aware social space.*
13. Michael Backes, Matteo Maei, and Kim Pecina. *Spac: a distributed, peer-to-peer, secure and privacy-aware social space.*
14. S.M.A. Abbas, J.A. Pouwelse, D.H.J. Epema, and H.J. Sips. *A gossip-based distributed social networking system*