International Journal of Scientific Research in Computer Science and Engineering
Research Paper Vol-1, Issue-3 ISSN: 2320–7639

Information Leakage through Social Networking Websites leads to Lack of Privacy and Identity Theft Security Issues

Ramesh Bandaru[1] and Rao S Basavala [#2]

[1] Dept. Of Computer Science, AITAM, Tekkali, India and Email:
[#2] Application Security Specialist, Bangalore, India and
Available online at www.isroset.org

Received: 28 March 2013 Revised: 15 May 2013 Accepted: 08 June 2013 Published: 30 June 2013

***Abstract*—** Social Networking Websites (SNW) such as Facebook, Orkut and Twitter etc., have gained more attractiveness in recent days. Because of its large number of usage, and large amount of information, they become a potential network for malicious users or attackers to exploit. Most of the social networking websites try to prevent those exploitations, but many malicious users or attackers are still able to overcome those security countermeasures by using different prevention techniques. Social network website end users may not be aware of such potential threats. Unfortunately, social networking is also common with their own security and privacy policy issues which stance a challenge for organizations trying to balance the benefits of social networking with the risks and it can pose to network and data security. Therefore, this paper will present a different privacy and security issues in online social network websites. The SNW issues include privacy issues, identity theft or personal information leakage, social networks spam and physical threats.

***Keywords*—**social network website privacy issues, social network website security issues, social network threats, identity Theft, social network spam, social network malware, Facebook and Twitter security issues.

I. Related Work

Social Network Website Services (SNWS) have paying attention of both organizations and researchers in recent years. Basically, from an academic view point, the services provide the R&D community with an exceptional opportunity to study the structure and properties of social networks. SNW user interaction and relationships in social network services have also been studied by researchers. SNW services from the standpoint of human factors, and they found that knowledge of, or trust between SNW users is not required to establish online relationships. Moreover, it has been given away that online social networks stimulate much weaker bonds between users than their offline activities.

Based on some SNW profiles gathered from Facebook.com, researchers analyzed the degree of personal information disclosure and the subsequent risks [1]. Also, researchers found that SNW users' personal data is provided, and preventive privacy preferences are hardly used. The privacy issues raised by SNW services present a difficult challenge to both information technology and social science researchers.

II. Introduction

Social Networking Websites (SNW) such as Orkut, Facebook, Twitter and MySpace has been increasing rapidly within the past few years and now more than two billions users are using. Almost every computer literate user has at least one social network site account, and every user spend a large amount of their valuable time on social networks sites each day [3] [5]. In the todays we can see different kinds of social networking sites as shown in the Figure 1.

Corresponding Author: *Rao S Basavala*

Figure 1: Different social networking websites

Social network websites can be termed as normal web applications that allow users to create their semipublic profile i.e. a profile that some information is available to public and some is private, communicate with those who are their network connections (called as friends), and they form an online community. It is based on social relationships among the users [10] [11]. Most people join in social networks websites to share their information and keep in connection with people they already know. The key feature of social network sites is a friend or colleague finder that allows social network users to search for people that they already know and then form their own online community as shown in the Figure 2.

Most of the social network users share a large amount of their private information such as date of birth in their social network space [13] [14]. This information includes from demographic and geographic information, contact information, comments, images, videos, etc.

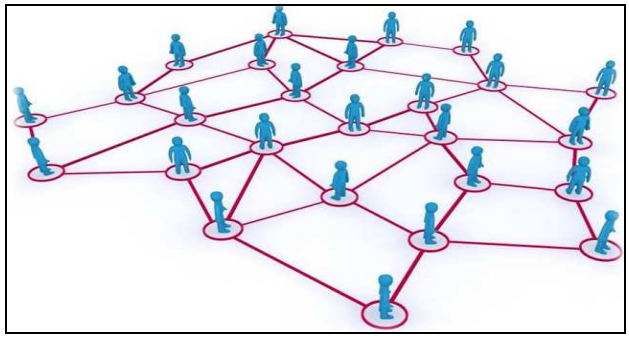

Figure 2: Social network users known friends connections

In the recent day's usage of social networking increasing rapidly. There are many reasons as follows:

- To expand you're your network
- Using your friends' friends
- Market to your community
- Understand your counter-part
- Watch your competition
- Create your own opportunities
- Discover the one-in-million
- Manage your image
- Use it within the company

With these characteristics of social network sites and the more forcefulness of attacker's methods, privacy and security issues in social network usage has become a critical issue in the cyber world. Therefore, in this paper we will present a survey on privacy and security issues that happen in social network websites. Also, we will discuss good and bad about SNW. The issues include privacy issues, identity theft issues, phishing issues, spam issues, malware issues, and physical threats issues [12]. The last section will be the conclusion or summary of the paper.

III. Attack Methods

Many social network users publish their information publicly without careful consideration. Hence, social networks have become a large pool of user's sensitive data. Moreover, social network users have a tendency to to have a high level of trust towards other social network users. They have a habit of to accept unknown friend requests easily, and trust items that friends send to them.

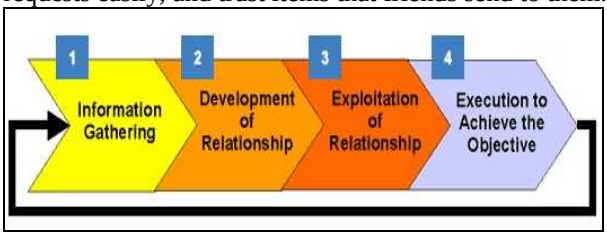

Figure 3: Social engineering attack cycle

As shown in the above Figure 3, an attacker uses a systematic approach to get the victim personal information. To achieve this they have multiple methods as discussed in this section.

Because of social networks sites large population and information base, and its' simple accessibility, social networking websites have become new objectives that attract lot of cyber criminals [15]. Cyber criminals or attackers exploit users sensitive data and chain of connection mostly through social engineering techniques and reverse social engineering (RSE).The goal of these two approaches is to obtain user's context-information i.e. information that is associated or meaningful to social work users. Both approaches are being used prior to other attacks such as phishing, spear phishing, spamming [19] and different malware attack. In social engineering, malicious users or attackers approach user's accounts and extract user's context-information then use this information to increase successfulness of their attacks [11]. On the other hand, in the reverse social engineering approach, attackers will not directly approach social network users. Attackers will try to trick SNW users to initiate a contact with them or encouragement users to accomplish some actions.

There are three approaches to implement RSE [17]. The first one is recommendation-based reversal social engineering. This approach makes use of friend recommendation feature to introduce attackers to the victims (social network site users). The second approach is demographic-based reversal social engineering. This approach is also established on friend recommendation feature that exploits victim's demographic information such as user's locations [13] and interests etc. The last approach is visitor-tracking based reversal social engineering. This approach is based on the social network site visitor tracking feature of some or all of the social networks websites. This feature allows social network users to find out who have viewed their profiles. Malicious users or attackers can use this functionality to make victims notice them, and visit their profiles. The main aim of the attackers is to collect as much information (personal information) as possible as shown in the Figure 4.

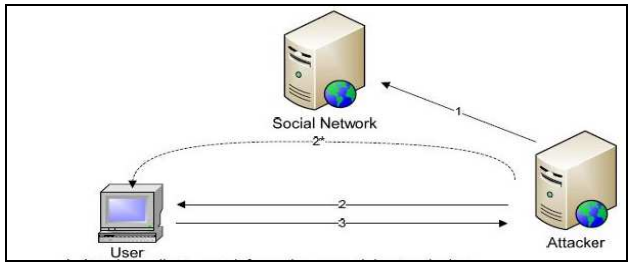

Figure 4: Attacker collects the user's personal information.

1. Attackers collect personal information from social network sites
2. Send fictional message / construct application with personal information
3. Collect additional personal information

Social networking websites or services have taken the internet by tempest. For example a social network site Facebook has more than half a billion members from around the globe. Another SNW Twitter, smaller in membership than Facebook [23] is the other leading social networking service. Its short, 140 character maximum status updates can be posted from the web by their users, as well as through short messaging services (SMS) text messages from any mobile phone have established. The SNW Twitter as a go-to source of transgression information. During the national elections in Iran, Twitter remained as essentially the only reliable source of current events. Recently in Syria, Twitter had remarkable impact on the liberation of the Syrian people [6] [16].

The Bad, Good and the Balance: Social networking websites can be an effective instrument for communication throughout the globe with in short span of time. If they used properly, it allows individuals and organizations to stay engaged with a large number of people instantaneously. A status update is instantly shared with hundreds of SNW users, or even thousands of members

connected to your social network sites. That is great when letting friends and family know that you enjoyed. However, it also gives a risk that user sensitive information can be leaked with much greater speed and efficiency as well. For example a social network user might send his Social Security Number (SSN) to another user might be his friend, and accidentally transmission it to the whole social network group users instead so, it is very bad [9].

A study report titled social insecurity revealed some informative data about the risks associated with social networking sites. Some of the key discoveries include:

- An estimated 5.4 million online users submitted their personal information to email (phishing) scammers during the past two years.
- Among adult SNW users, more than 38% had posted their full personal details like birth date, including birth year. 45% of those with children had posted their children's photos. And 8% had posted their own postal address.
- On an estimated 5.1 million online social network households had experienced some type of abuse on a social network in the past year, including malware infections, scams, and harassment and many more.

IV. SOCAIL NETWORK WEBSITE SECURITY ISSUES

A. Privacy and Security Issues

In this section, we will discuss two privacy issues [18]. The first is SNW user's anonymity or user's identity. There are two approaches of identifying SNW users identities in social networks sites will be described. The second issue is user's profile details and personal information leakage. This may leads lot possible attacks on SNW users in the real time not only from information security stand point and also physical attacks.

In many social networking websites [9], end users use their actual name (real name) to represent their accounts. So, their identity is publicly exposed to other social network site users or groups, and everyone else in the social network site. Also, social network site user's account can be indexed by search engine and usually appeared in the top rank of the search results. In this case, if attackers know the name of the victims (social network users), they can easily search for victim's profile or they can search through social networking sites to obtain new victims. Apart from the simple use of SNW real name as account name, there are also other techniques that can be used to expose social network user's secrecy. The two methods that will be discussed are deanonymize attack and the neighborhood attack.

a) De-Anonymization Attack: A group of researchers showed that by using group membership information and history stealing technique, attackers could reveal anonymity of any social network users.

In this technique, what attackers need to learn is in which social network group (group of SNW users that shares similar interests or group of people with same background e.g. studied to same school or same work place etc.) the victims belong to. The social network group is being dedicated since the number of a social network individual user is a lot larger than the number of groups in social networks. Hence, it is very easy to first concentration on the group, and then uses the group to access each individual user. All most all the attackers will use history stealing method to get which URLs (websites) that targets (victims) visited in the past to find out victim's group. Before going through, how this technique works and concepts of social network and history stealing will be described.

There are two types of links in SNW. A static content link is the same across all social network users. This is used for displaying user's home page, and a dynamic link that contains some information unique to each individual user or each individual group. For e.g. dynamic link looks like: http://www.facebook.com/groups/groupID/

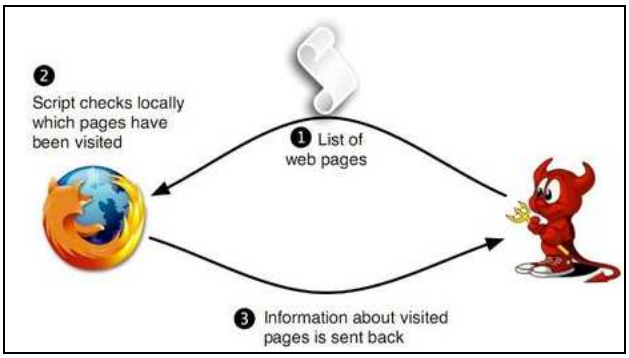

Figure 5: An overview of stealing attack

In history stealing as shown in the above Figure 5, attackers pull users to their web pages, and then they try to extract user's browsing history by sending out a list of URLs i.e. URL of social network website group that users probably be part of. These URLs can be obtained easily through group directory provided by social networking websites. Then, attackers will make victim's web browser to check whether any URL on the list was visited by victim (SNW user) or not by looking at victims' browsing history. Then, the browsing history is sent back to attackers. Pulling out of user's browsing history can be done by using provisional logic in cascading style sheet i.e. a: visited and display: attribute" or using client side java script. Therefore, by using history stealing, attackers can get victim's browsing history, and then use this list to riddle out URLs that are related to victim's activity in SNW, especially the dynamic social network URLs that contain some distinctive info about SNW users or groups. In general, many social network groups provide mailing list of the group members. So, attackers can use get emails to search for identity (users' profile) of victims.

b) Neighborhood Attack: Social networks sites can be represented by social graph where a simple node represents a social network site user, and an edge represents relationship between two SNW users. A neighborhood attack is based on the idea that if attackers know the neighbors of the victims' node, and the relationship between them, then attackers can identify

victims' node. For example, if an attacker knows that user A has five friends, two of A's friends (B, C) are friends with each other and the other three (D,E,F) are not friends, Figure 6 shows one-neighborhood graph of user A. Attackers can use this graph to identify A since one-neighborhood graph is unique to each social network user node.

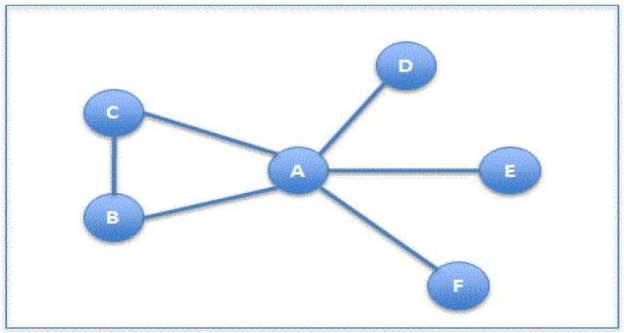

Figure 6: 1-Neighborhood Graph of A

B. User's Profile and Personal Information

As we know social network user information publically available to online users. SNW user's account, social network user's profiles mostly contain actual information about SNW users. SNW users' sensitive information such as user's first name, last name or full name, contact details, relationship status, date of birth, previous and current work and educational information attracts attackers. Hence, the major issue of user's profile is the leakage of users profile and personal information. We can see sources of SNW users' profile leakage are:

a) Sensitive information leakage through poor privacy policy: Most of the social network users are not cautious about their privacy settings. Many of SNW users open their profile to the general public so anyone can access and see their information including date of birth. Also, many social networking websites default privacy settings are still not safe such as in Facebook or Twitter, a friend of a friend who the user does not know can still see his information. However, even the safest privacy setting, there are still flaws that allow attackers to access user's information.

b) Sensitive information leakage to the third party applications: Many SNW such as Facebook (FB) provides an Application Programming Interface (API) for 3rd party developers to develop and create applications that can run on its platform. These applications are so popular at the social network users' world. Once SNW users add and allow these 3rd party applications to access the information, also, these applications can access user's data automatically without knowing to social network users. These apps also capable of posting on users' space or user's friend's space, or may access other user's data without user's knowledge.

c) Information leakage to third party domain: Most of SNW uses third party domain service is used to track social network user's activities in their site, or it allows advertisement partner to access and aggregate social network user's data for their profitable or commercial benefit.

C. Identity Theft

Identity Theft is an act of stealing or theft someone's identity or sensitive information, and then play-acting to be that person, or by using that identity in a malicious way or different purpose. Social network sites are favorable targets that attract malicious users or attackers since they contain a huge number of available user's profiles and their information. There is always one method of identity theft is SNW profile cloning. In this method, an attacker take benefit of trust among friends, and those people are not very careful when they accept friend requests. Social phishing attack [24] is another technique that can be used to theft or steal social network user's identity. As shown in the Figure 7, most SNW real names compromised based on their age.

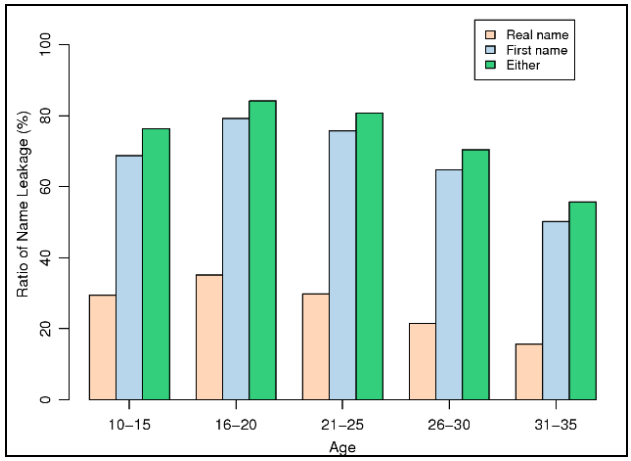

Figure 7: Real name leakage based on age group

a) Threats Caused by Name Leakage:
In the recent years, spamming or also called as spam mail has become a bigger problem. This kind of activities is actually a business activity whereby spammers send emails with some product information based on huge email address lists. In effect, any user who has an email address listed in the list is regarded as a potential customer (actual victim). To protect users from this kind of spamming attacks [25], academia and industry have developed a different kind of approaches of anti-spam mechanisms. One common technique of protection against spam includes using a white list, so that emails from trusted business parties will not be mistaken for spam. However, as spamming emails is profitable, spammers are always formulating new ways to enter spam filters. In the white list approach, spammers collect email ids and the information about social relationships from social network services. In this way, spam mail can bypass the filter and be delivered to the target's victim's mailbox [19].

Spammers may use of real names in two ways:
1) They may use the receiver's real name in the mail's content.
2) They may make spam mails look like they have been sent by a friend of the target by using the friend's real name [21].

Consider an email containing the receivers' real name, where the sender (spammer) is specified as a friend with

his or her correct email address and real name. The user may have difficulty in verifying the email's genuineness.

b) Phishing:

There are similar problems also persists with respect to phishing attack detection. Phishers usually send emails, which contain a URL or direct link to a forged web page or site, to obtain people's sensitive information, such as an account or user ID, social security number (SSN) or credit card number. Some phishing targeted companies, including eBay and PayPal [22] [26]. Actually, internet security vendors provide guidelines for recognizing phishing emails. Common rules include checking if the email contains your real name because phishers do not have personal information. However, the assumption that phishers do not have Personal or profile information might be incorrect as self-disclosure is becoming more common in social network service sites. The spontaneous name leakage problem will make worse the problem further, as it will be very difficult to users and phishing detection techniques to verify the authenticity of a web page.

c) Profile Cloning:

Common method of stealing social network user's identity is also called profile cloning. The main targets of profile cloning attacks are users who set their profiles to be general public. Public profile information leakage as shown in the Figure 8 allows attackers to obtain profile information easily, and therefore can make duplicate [24] or copy their profile information to create a false identity. There are two types of profile cloning.

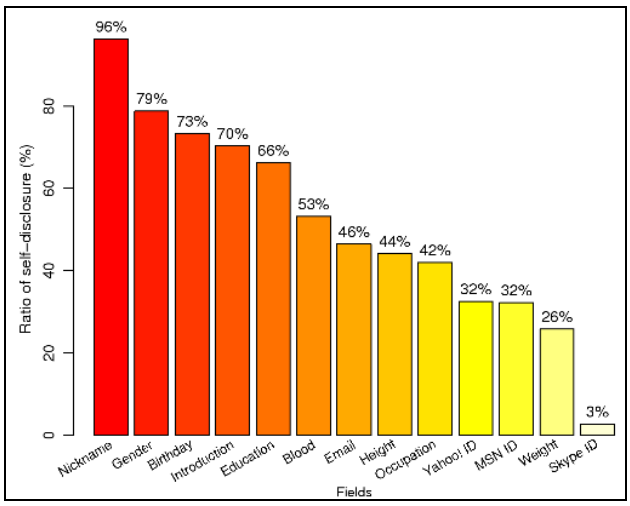

Figure 8: self-disclosure. The name, gender and birthday profile information have a high disclosure

i. Existing or Persisting Profile Cloning: In existing profile cloning, a malicious users or an attackers can create a profile of registered users by using their name, personal or profile information [20], as well as picture to increase confidence, and then distributing friend requests to friends of that user (victim). If this action is success since most of the SNW users accept friend requests from the person that they already know without looking through it carefully. Also, it is possible that a person might have multiple accounts. If victims accept the friend requests, then attackers will be able to access their entire profile information.

ii. Cross-Site Profile Cloning: In cross-site [4] profile cloning, malicious user or attackers steal user's profile from one social networking site that users register an account, and then create a new user's profile on another social networking site that user has not registered on before. After that, attackers use users contact list from the registered social networking site to send a friend requests to all those contacts in another social networking site. In this case, it is more convincing than the first case since there is only one account for that particular user. Then, if the contacts accept friend request, attackers can access their profile.

d) HTTP Session Hijacking:

HTTP (Hyper Text Transfer Protocol) session hijacking [2] [7] [8] is type of session management attack (OWASP - top10) on social networking sites it can be used to obtain context-information such as cookies from victims, as well as victim's friend's information that will later be used to generate context-aware spam.

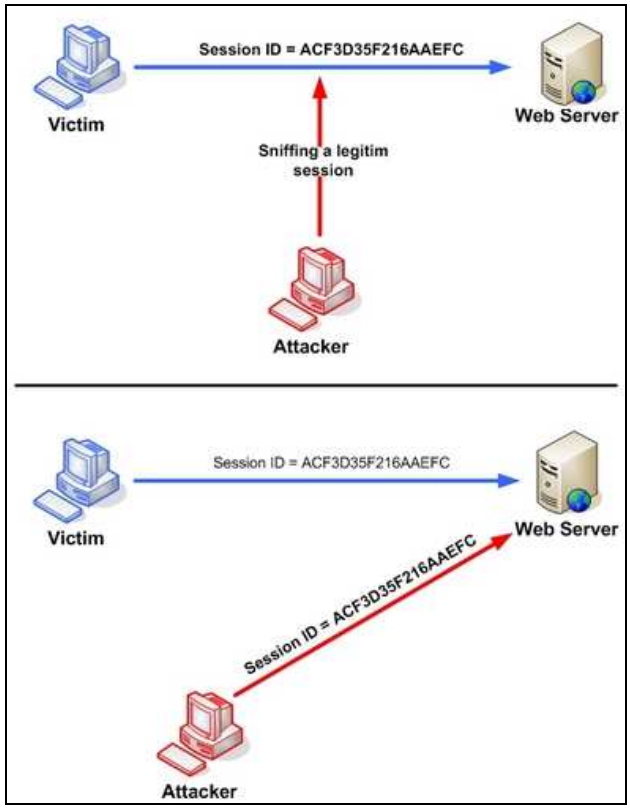

Figure 9: Influencing the token session executing the session hijacking attack.

As shown in the above Figure 8 proves it how session hijacking attack works on social network users. Firstly an attacker tries to sniff network communication between victims and social networking websites, mainly those without using data encryption. There can be multiple network attacks can be used in this case, for example, ARP cache poisoning or DNS poisoning. Attacker captures HTTP headers that contain user session cookies since many social network websites and commercial websites use session cookie-based authentication. After that

attackers now copy the HTTP session-ID and use it to access the victim's profile information includes personal details. Moreover, attackers use the victim's profile to retrieve the victim's friend's information such as email addresses, and then use this information to generated spam based attacks.

D. Physical Threats

As we discussed different type of attack vectors which may cause to SNW users. In addition to online threats that lead to social network users, physical threat is another issue that social network users need to concern physical threats too. Physical threat is physical harm to a person, or to a person's property such as theft, stalking, blackmailing, or even physical harassment. With the characteristics and features provided in the social network websites, social network users at risk of such threats. So, social network users should think before post their personal information and that information availability publically

The first characteristic of the social network user's real identity is not known or not genuine. Hence, we do not know who we are connecting with in friends group. The second characteristic is the personal information that is posted on the social networking websites that include user's contact information like mobile number [6], email ids, and their interests, habits etc., this information will allow criminals to easily learn about and approach victims. Moreover, many of the security issues which we mentioned here can also lead to physical threats. For example, social phishing attacks may allow attacker to physically access a victim's bank account, and perform some transactions. Privacy issues are also another threat that can lead to physical threat. If criminals can access some sensitive information such as a sensitive picture or video post, they can use them to blackmail victims.

In addition, many social network features allow cyber criminals to be able to track victim's behavior, day to day activity and location. For example, location-based services on smart phones such as Google Latitude or Foursquare, allows social network users to check in and post their current location onto their message board. Also, if social network users use social network application on their smart phones to post something, their jagged location will also be posted. Moreover, another feature such as GeoTag (in security called geo tagging attack) that allows users to tag their location [24] on the image that they post can also expose user's location, so followers or cybercriminal will easily know where the victims are, and can approach them.

Along with different security issues which we have discussed above, there are other security issues also listed in the below:

- Harassment
- Peer pressure
- Loss of employment
- Damaged business reputation
- Damaged career or personal reputation
- Damaged data or networks
- Intellectual property theft / Data theft
- Brand hijacking
- Delays or interruption in production
- Lost revenue or income
- Content alteration of websites
- Malware and virus dissemination

V. CONCLUSION

In the recent years social networking websites have become a potential target for attackers due to the availability of huge sensitive, personal and profile information, as well as its large user base. Therefore, privacy and security issues in online social networks are increasing. This paper speak to different privacy and security issues, as well as the techniques that attackers use to overcome social network security mechanisms, or to take advantage of some flaws in social networking web sites.

Privacy issue is one of the main anxieties, since many social network users are not careful about what they expose on their social network space. The secondary issue is identity theft; attackers make use of social networks account to steal victim's identities. Also an attacker makes use of social networks to increase spam click through rate, which is more effective than the traditional email spam issues and attackers use social networks as a channel to spread malware, since it can spread very fast through connectivity among users. We can also see physical threats, which are the most harmful issues, were addressed. Because of some of the social network features such as location-based service, it is easier for cybercriminals or criminals to track and approach victims.

Social networking websites try to implement different kind of security mechanisms to prevent such issues, and to protect their registered users, but malicious users or attackers will always find new attack scenarios to break through those defenses. Therefore, every social network users should be aware of all these threats, and be more careful when using them.

REFERENCES

[1] ENISA: Enisa position paper no.1, security issues and recommendations for online social networks http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

[2] IETF,RFC2109: HTTP State Management Mechanis http://www.ietf.org/rfc/rfc2109.txt

[3] Gross, R., Acquisti, A., Heinz III, H.: Information revelation and privacy in online social networks. In: Proceedings of the 2005 ACM workshop on Privacy in the electronic society, ACM Press New York, NY, USA (2005) 71-80

[4] The Open Web Application Security Project,Cross Site.Scriptinghttp://www.owasp.org/asac/input_validation/css.shtml

[5] Ahn, Y., Han, S., Kwak, H., Moon, S., Jeong, H.: Analysis of topological characteristics of huge online social networking services. In: Proceedings of the 16th international conference on World Wide Web, ACM Press New York, NY, 835-844

[6] Mislove, A., Marcon, M., Gummadi, K., Druschel, P., Bhattacharjee, B.: Measurement and analysis of online social networks. In: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, ACM New York, NY, USA, 29-42

[7] The Open Web Application Security Project, Session Hijacking. http://www.owasp.org/asac/authsession/hijack.shtml

[8] David Endler, »Brute-Force Exploitation of Web Application Session ID. http://online.securityfocus.com/data/library/SessionIDs.pdf

[9] Kumar, R., Novak, J., Tomkins, A.: Structure and evolution of online social networks. In: Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, ACM Press New York, NY, USA. 611-617

[10] O¡¦Murchu, I., Breslin, J., Decker, S.: Online social and business networking communities. In: Proceedings of ECAI 2004 Workshop on Application of Semantic Web Technologies to Web Communities.

[11] Boyd, D.: Friendster and publicly articulated social networks. Conference on Human Factors and Computing Systems (CHI 2004), Vienna, Austria, April . 24-29

[12] Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM conference on Electronic commerce, ACM Press New York, NY, USA. 21-29

[13] Jourard, S., Lasakow, P.: Some factors in self-disclosure. Journal of Abnormal and Social Psychology 56(1) 91-98

[14] Ajzen, I. (1991). The Theory of Planned Behaviour. Organisational Behaviour and Human Decision Process, 50(2), 179-211.

[15] Joinson, A.N., Paine (Schofield), C. Oxford Handbook of Internet Psychology. In: Self-Disclosure, Privacy and the Internet. Oxford University Press 237-252

[16] Farmer, R.: Instant messaging-collaborative tool or educator's nightmare. In: The North American Web-based Learning Conference.

[17] Judge, P., Alperovitch, D., Yang, W.: Understanding and reversing the profit model of spam. In: Workshop on Economics of Information Security.

[18] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523-548.

[19] Oscar, P., VWANI, R.: Personal Email Networks: An Effective Anti-Spam Tool. IEEE Computer 38(4) 61-68

[20] Carvalho, V., Balasubramanyan, R., & Cohen, W. (2009). Information Leaks and Suggestions: A Case Study using
Mozilla Thunderbird. Paper presented at the CEAS 2009 - Sixth Conference on Email and Anti-Spam.

[21] Seigneur, J., Dimmock, N., Bryce, C., Jensen, C.: Combating spam with TEA (trustworthy email addresses). In: Proceedings of the Second Annual Conference on Privacy, Security and Trust (PST¡¦04). 47-58

[22] Garcia, F., Hoepman, J., van Nieuwenhuizen, J.: Spam Filter Analysis. In: Proceedings of 19th IFIP International Information Security Conference, WCC2004-SEC, Kluwer Academic Publishers.

[23] Facebook. (2010). Facebook Statistics. Retrieved 14 Sept 2010, from http://www.facebook.com/press/info.php?statistics.

[24] Zhang, Y., Egelman, S., Cranor, L., Hong, J.: Phinding phish: Evaluating anti-phishing tools. In: Proceedings of the 14th Annual Network and Distributed System Security Symposium.

[25] Microsoft.com: Recognize phishing scams and fraudulent emails. http://www.microsoft.com/athome/security/email/phishing.mspx.

[26] PayPal: Phishing guide part 2 https://www.paypal.com/us/cgi-bin/webscr?cmd=xpt/cps/securitycenter/general/RecognizePhishing-outside.

[27] Wu, M., Miller, R., Garfinkel, S.: Do security toolbars actually prevent phishing attacks? In: Proceedings of the SIGCHI conference on Human Factors in computing systems, ACM Press New York, NY, USA. 601-610

AUTHORS

Ramesh Bandaru has completed B.Tech (CSE)., M.Tech (CSE). He is currently working as a Asst.Professor in Aditya Institute of Technology And Management (AITAM), Tekkali. He has over 6 plus Years of experience in IT industry and Academic. His areas of interests are Web Technologies, Web Security, Software Engineering, Mobile Application Development and Databases. His area of research interest is Web Application Security, Security code reviews.

Dr. Rao S Basavala has completed M.S (CS)., M.Tech.(IT), Ph.D. (CSE)., also he has done java certifications such as SCJP, SCWCD and IBM-ACSE, and he is currently working as a Sr. Application Security Specialist in one of the core and online banking product development IT company in Bangalore, India. He has over 11 plus years of experience in IT industry and Academic. His areas of interests are Web Application Security, information Security, Software Engineering, Computer Networks, Cryptography, Mobile Application Security, Database Security, DBMS and RDBMS. His area of research interest is Web and Mobile Application Security, Security code reviews and Penetration testing in various financial and retail domains.

