An Overview of Privacy and Security in SNS

Rashmi A.Zilpelwar, Rajneeshkaur K.Bedi, Vijay M.Wadhai
Department of Computer Engg, MITCOE- Pune University, India
Department of Computer Engg, MITCOE- Pune University, India
Principal, MITCOE –Pune University India

Abstract— The use of Social Networking web sites and applications is rising day by day, many users are not properly informed of the risks associated with using these sites and application. User should understand these risks and challenges to avoid potential loss of private and personal information. Here we are examining the issues of security and privacy. There are many attacks possible on social networking sites and those can be used to collect social data in an automated fashion. Attackers can then make use of this data for large-scale attacks using context-aware spam and social phishing. Here we are discussing the feasibility of such attacks and simulate the impact on social networking sites. Frighteningly, all major social networking sites are susceptible to this attack because they fail to appropriately secure the network layer.

Keywords— Social Networking Sites.

I. INTRODUCTION

Social Networking Sites have exponentially grown in popularity in the recent few years.

A. Definition of SNS

As defined by [1] social networking sites as web-based services that allow individuals to: construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system. Social Networking Sites allow users to connect, share information and other contents, chat, play games, and even add comments.

Some social networking sites may require specific protocols to allow interaction among members, while other social networking sites allow open interaction among all site members. At any point, users should be informed of the information security threats and challenges they could be exposed to, including the potential loss of private and personal information.

B. Types of SNS

There are many types of SNS sites are available, for Business, Healthcare, Music, General, Mobile, Media and even for Dogs and Cats etc. SNS vary greatly in their features. Some have photo-sharing or video-sharing capabilities; others have built-in blogging and instant messaging technology etc. Some sites are designed with specific ethnic, religious, political, or other identity driven categories in mind. While SNSs are often designed to be widely accessible, many attract uniform populations initially, so it is common to find groups using sites to separate themselves by nationality, age, educational level, or other factors.

Best social networking sites as given in [2], which could probably provide you with more networking options. All of these SNS are having some similar features like find friends with similar interest, share lists of contacts, comments from friends and other users, post blog entries for others to read, social networks usually have controls that allow users to choose who can view their profile, contact them, add them to their list of contacts, and so on.

Facebook has many applications like superpoke, photo albums, gifts, books, music, movies and games. MySpace main features include Bulletin board, Group, TV, Classifieds, Karaoke, Polls and forums. Twitter enables its users to send and read messages called tweets. Flicker is the most popular image and video hosting and sharing website. Bebo is the largest social networking site in the UK, Ireland, and New Zealand, and the third largest in the United States. LinkedIn is a fast growing business oriented social networking website. LiveJournal can be used as a private journal, a blog, and much more. Ning enables users to create their own social network for a particular topic or need. Hi5 is extremely popular among Thai people and Orkut.

1)Healthcare related SNS: Doctors, surgeons, nurses and students all can gain valuable connections and invaluable knowledge by joining one of social networking sites for healthcare and medical professionals given below.

Healthcare related SNS as given in [3] are Doc2Doc, DocCheckFaces, Doctornetworking, Healtheva, Ozmosis, Relaxdoc, StudentDoctorNetwork.

2) Music related SNS: Sharing your musical taste with others is a fun way to discover new music and friends too. Some of the best social music sites given in [4] for music sharing and listening to your friends music are Meemix, Meastro.fm, Last.fm, Pandora, WorldSings.

3) Business related SNS: You can easily build accounts with each of them, along with our personal ranking chart. These SNS sites can help you begin expanding your business. Most popular as given in [5] Business related SNS are Facebook, Twitter, Digg, delicio.us, Stumbleupon, Current, Propeller, Diigo, Ezinearticles, Ning.

C. *Purpose of SNS*

Most social networking sites offer the basic features of online interaction, communication, and interest sharing, letting individuals create online profiles that other users can view, it also allows users to post a rich variety of information and to establish relations with numerous online friends and contacts. It also allows users to share ideas, activities and events within their individual networks. Social networking sites share some usual features. Most often, individual users are encouraged to create profiles containing various information about themselves. Users can often upload pictures of themselves to their profiles, post blog entries for others to read, search for other users with similar interests, compile and share lists of contacts. In addition, user profiles often have a section dedicated to comments from friends and other users.

II. SECURITY OBJECTIVES IN SNS

The three main security objectives [20] of SNS are privacy, integrity and availability, which come in considerably different way than in usual systems.

A. *Privacy*

Privacy has to be met by default that is, all information of all the users and their actions has to be concealed from any third party internal or external to the system, except clearly reveal by the user. In accordance to previous studies [21,22] we assume the protection of the user's privacy to be the main objective for SNS.

B. *Integrity*

The user's identity and data must be protected against unauthorized modification and interference. The concept of integrity comes with conventional modification, detection and message authentication, now it needs to be extended in the context of SNSs, the creation of person's fake accounts, cloned accounts, or other types of impersonation. Many users have a strong intrinsic trust in SNS. This combination of trust and impersonation may lead to new kinds of vulnerabilities. In consequence, the authentication has to ensure the existence of real persons behind registered SNS members. Identity checks do not necessarily have to be performed by a centralized service; however, all identification services have to be trusted by all participants.

C. *Availability*

Availability of user profiles is consequently required as a basic feature, even though considering recreational use, the availability of some content may not seem a severe requirement. Some SNS are used as professional tools to aid their members, business or careers, data published by users has to be continuously available. In SNSs, this availability specifically has to include sturdiness against censorship, and the spasm or hijacking of names and other key words. Apart from availability of data access, it has to be ensured along with message exchange among members.

III. THREATS TO SECURITY AND PRIVACY

Many users strongly believed that SNS will protect their information privacy and will not sell it to third party, although they never read the website use/license agreement and many people believe that information shared in SNS is meant to be public not confidential and should be seen by other members within that site. The key concern in general is, the privacy of some personal information is required, including contact information and financial. Many kinds of attacks are possible on SNS.

As characterize by [23] major attacks on SNS are

A. *ID theft*

The important aspects that still need to be addressed is the protection of a member's identity in SNSs. In identity theft an attacker or service provider gain the identification of authorized users and acts on their behalf with full access to the profile, friends, and communication traces.

B. *Profile cloning*

Generally user have natural trust in other profiles, the attacker can impersonate the user by creation of a clone of the targeted profile which may be enough to be able to establish trust relationships with parties on a user's contact list by simply sending new friendship requests.

C. *Profile porting*

In Profile porting attacks, the attacker make use of the user's identity and creates a profile in an SNS where the user is not present, so they are more difficult to detect. Most existing accounts are generally unprotected. So, profile porting pose a valid threat.

D. *Secondary data collection*

User published the data on an SNS, so using this data attacker may easily be able to guess the social security number, which often acts as a key to accessing personal information from a wide range of different sources. Generally people are having account in profession related SNS (like LinkedIn) and informal SNS (like Facebook), matching the profiles of a person for analysis and comparison of the content published in both is another obvious and frequent type of secondary data collection.

E. *Communication tracking*

A series of other threats arises when moving from data to communication privacy. A malicious SNS provider or a malicious member with the appropriate set of privileges can be able to perform communication tracking and reveal who is talking to

whom. This problem is very relevant and difficult to solve.

F. Image retrieval, Face recognition

Image retrieval comes in the form of more sophisticated collection of data, possibly even in association with automated face recognition algorithms for further profiling. The impersonation attacks are due to a basic limitation, in many cases the current major SNSs is unable to ensure that a profile is associated with a single real person.

G. Sybil attacks

Bogus profiles are a common observable fact resulting from this limitation. Such impersonation gives the way for Sybil attacks, which aim at creating fake identities

H. Defamation and Ballot stuffing

These attacks aim at disturbing the reputation for a person using the system .

I. Friend-in-the-Middle-Attacks

This attack is very well explained by [12,13,15].This attack hijack HTTP sessions on the network layer, which the majority of SNS providers fail to secure. This attack can also hijack session cookies, an attacker can impersonate the victim and interact with the social network without proper authorization.

An attacker can access communication between the SNS and user. They clone the HTTP header containing the authentication cookies and can interact with the social network, unbeknownst to the SNS operator or user. Scenarios that are specific to SNSs are:

1) Friend Injection: The basic security and privacy protection measures of SNSs available to users are based on the concept of "friendship," which means that sensitive information is made available to only a limited set of accounts (friends) that the SNS user specifies. The attackers hijack a social networking session, and then they can add themselves as friends on behalf of the victim and thus penetrate the target's closed network. The injected friends can then be misused to access profile information or to post messages within the infiltrated network of friends.

2) Application Injection: Third-party applications, such as online games, are popular on SNSs, and hiding a malicious application without any activity visible to the user is possible. An attacker could install an application, take all the data needed in an automated fashion, and then remove the application without the user, and possibly the SNS provider, detecting it. By writing, installing, and controlling a custom third-party application, the attacker can access data in an automated fashion — data such as the user's birth day, pictures, gender or activity. With most SNSs, the application might also have access to information about the user's friends.

3) Social Engineering: Social engineers have traditionally depend on related information gathered through dumpster diving or quizzing people over the phone, FITM attacks mechanize the Context-information harvesting process. FITM attacks thus allow sophisticated social engineering attacks. Consider the following two attacks based on information extracted from SNSs.

- *Context-aware spam:* Three types of attacks can generate this data, association based (based on relationship information) unshared-attribute and shared-attribute (based on content extracted from SNSs such as phone number or user's place).
- *Social phishing*: An attacker tries to attract victims into entering sensitive information, such as a password or credit-card number, into a bogus website that the attacker controls. Social phishing make use of social information specific to the victim and is thus more effective than regular phishing. For example, the attacker may appear as a friend of victim's social environment.

With the help of FITM attacks, attacker can gather a vast amount of information related to user. The information could include user post, photos, messages or comments. Using this information, attacker could increase a phishing email's authenticity. Email could include the photos from targeted user's account and a link that would lead to more pictures if user enters his or her social networking official document. Spam and phishing message via Friend-in-the-Middle-Attack can be delivered using one of the various approaches: The social network itself might be used for sending the spam or out-of-bound spam messages: that is an attacker uses traditional emails to deliver the spam or phishing messages.

IV. CONCLUSION

The majority of SNS users are not properly informed of the basic security risks involved while using social networking sites. Many of the examined users admitted to sharing their passwords, or accounts with others. While others could not identify basic information security risks such as phishing, and spam email. We suggest SNS users to use a tool called Privometer, which measures privacy leakage in social networks including information obtained by malicious applications installed in the user's friend profiles. Privometer ranks friends based on their individual contributions to privacy leakage and suggest self-sanitization to reduce this leakage accordingly.

Social networking providers need to protect their users against attacks by securing the communication channels of their services with

HTTPS, full HTTPS support is the obvious solution. We suggest that SNS sites should protect users from attacks using ,

- SNS sites can use better encryption techniques.
- They can make a use of Hippocratic principles, which are based on purpose concept and identify who can access our information, which information and for what purposes. On the way, it is also depends on owner preferences.
- Novel privacy-by-design ultimately help mitigate a number of known security attacks against SNSs, including FITM attacks.

REFERENCES

[1] Boyd, D., Ellison, N., "Social network sites: Definition, history, and scholarship." Journal of Computer-Mediated Communication, Oct 2007, Vol 13, no 1, pp. 210-230. http: //jcmc.indiana.edu/vol13/issue1/boyd.ellison.html

[2] http://topsitesblog.com/list-of-social-networking-sites/

[3] http://medicallabtechnicianschool.org/2009/top-25-social-networking-sites-for-healthcare-medical-professionals/

[4] http://mp3.about.com/od/digitalmusicdelivery/tp/Top-Social-Music-Sites.htm

[5] http://www.smashblogtips.com/10-top-business-social-networking-sites-on-the-web/

[6] Wikipedia, "Social Network Service," 2010; http://en.wikipedia.org/wiki/Social_network_service

[7] Zhang, C., Sun, J., Zhu, X., Fang, Y., "Privacy and Security for online Social Networks: Challenges and Opportunities" , IEEE Network , July/August, 2010, pp 13-18

[8] Furnell, S., Botha, R., "Social networks – access all Areas?", Communications and Network Research, South Africa, May, 2011,pp 14-19.

[9] "Facebook privacy settings to be made simpler". BBC News Online, 26 May, 2010.

[10] McKeon, M. 'The Evolution of Privacy on Facebook'. 2010. Accessed Feb 2011. http://mattmckeon.com/ facebook-privacy

[11] Freiert, M., "Facebook vs LinkedIn –Network, Socialize, Be Professional?", Compete Pulse, 22 July 2008 , Accessed Feb 2011, <http://blog.compete.com/2008/07/22/facebookvs-linkedin-traffic-demographics/>.

[12] Huber, M., Mulazzani, M., Kitzler, G., Gulch,S., Weippl,E. "Friend-in-the-Middle Attacks-Exploiting Social Networking Sites for Spam." IEEE Internet Computing, May/June, 2011, pp 28-34.

[13] Jones, H., Soltren,J., "Facebook: Threats to Privacy,", Dec, 2005, http://citeseerx.ist.psu.edu/viewdoc/summary?

[14] Brown, G., "Social Networks and Context-Aware Spam," Proc. ACM 2008 Conf. Computer Supported Cooperative Work, ACM Press, 2008, pp. 403–412.

[15] Huber, M., "Friend-in-the-Middle Attacks", tech. report TR-SBA-Research-0710-01, SBA Research, 2010; www.sba-research.org/wp-content/uploads/publications/ FITM_TR-SBA-Research-0710-01.pdf.

[16] Kritzinger, E., Smith, E., "Information security management: An information security retrieval and awareness model for industry", Computers & Security, 2008, vol. 27, pp. 224-231.

[17] Rezgui,Y.,Marks,A. "Information security awareness in higher education: An exploratory study," Computers & Security, 2008,vol. 27, pp. 241-253

[18] Vorakulpipat, C., Marks, A., Rezgui, Y., Siwamogsatham, S., "Security and privacy Issues in Social Networking Sites from User's Viewpoint", IEEE, 2011

[19] Vaidhyanathan, S., Welcome to the Surveillance Society", IEEE SPECTRUM. IEEE.ORG., June,2011, pp 49-51.

[20] Cutillo, L., Molva, R., "Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust" IEEE Communications Magazine, December, 2009, pp 94-101.

[21] Black Hat; http://www.blackhat.com/html/bh-usa-08/bhusa-08-archive.html

[22] Bilge, L., "All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks," 18th Int'l. W3C, 2009

[23] Boyd, D., "Facebook's Privacy Trainwreck," Convergence: Int'l J. Research into New Media Tech., 2008, vol. 14, no. 1, pp. 13–20.

[24] Talukder, N., Ouzzani, M., Elmagarmid, A., Elmeleegy, H., Yakout, M., "Privometer: Privacy Protection in Social Networks" ICDE Workshops, USA., 2010 IEEE, pp 266-269.

[25] Ghani, N., Sidek, Z., "Hippocratic Database: A Privacy-Aware Database" World Academy of Science, Engineering and Technology 42 2008, pp 549-543.