Privacy and Security Issues in Social Networks with Prevailing Privacy Preserving Techniques

Poonam Dabas
Assistant Professor, Department of Computer Science and Engineering,
University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, 136119, Haryana, India

Sheeba Sharma
M. Tech (Computer Engineering), University Institute of Engineering and Technology, Kurukshetra University, Kurukshetra, 136119, Haryana, India

Abstract – A social network is an online based network which allows users to interact with other users who share common interests and communities. Social networking sites(SNS) are very popular among users worldwide. Users who are connected to these sites exchanging their sensitive data with other users. So, various privacy and security methods are used for keeping the sensitive data more secure and eliminating the privacy or security issues. Due to the scalability of social networks, a complete elimination of privacy and security issues might be impossible. This paper is focused on various privacy and security issues w.r.t. social networks and various techniques proposed by various researchers in order to combat those issues.

Index Terms – Social networks; Privacy issues; SNS; security issues; privacy-preserving techniques;

1. INTRODUCTION

A Social network provides an online medium for building relationships between users. The trend of social networking sites is gaining popularity these days e.g. Facebook, LinkedIn, Twitter, Google+ etc. Billions of users are connected to these sites. Nowadays, Users' privacy and security norms are becoming a major concern. Each social networking site has its own privacy settings to alleviate the risk of leakage of users' sensitive information. The purpose of this paper is to analyze various privacy and security issues which arise in social networks and subsequently, discuss some prevailing privacy-preserving techniques in order to achieve anonymity and zero sensitive information leakage [1] [2].

2. SECURITY & PRIVACY ISSUES/THREATS

2.1. Spam

Spamming is a typical type of attack and It has affected almost every single technology which has ever existed. Emails, IM services, Gaming services etc., each of these has been affected by spam at one time or other. Social Networks are not absent from that list either. Spammers have been developing new techniques and modifying the existing ones in order to spam more effectively. Almost all social networks allow users to communicate with other users within their friend circle and some even allow users to communicate with the ones who are not in their friend circle. This has been exploited as an entry point for spammers. Spammers tend to create fake accounts or dummy accounts for this purpose. [3] [4]

Moreover, spammers have also been using the users' information available on the social networks in an effort to make spamming more effective and successful. They don't only get the contact information from the social networks, but they also get the identity information as well user's interests/likes. For example, if my profile mentions that I'm a luxury automotive enthusiast, I may be keen on clicking on a spam link mentioning cheap luxury cars.

2.2. Phishing

It is an attack which is executed by phishers to obtain sensitive/ financial information (including usernames, passwords, credit card details etc.) from a user. In phishing, the adversaries either use fake but identical websites in hopes to fool the users into entering their sensitive information like passwords. After getting such information, phishers can gain access to users' banking accounts or email accounts. [5]

2.3. Cyberbullying on Social Networks

Nowadays, Social networking sites are playing an important role in everyone's life. Social network gives us a platform where users interact with each other and form relationships as well. Unfortunately, there is a major concern referred to as cyberbullying, common in networking sites. Cyberbullying attack is very common among teenagers who are not sure of the options they are using. It's more of a social threat but social networks' privacy policies may turn out to be the ammunition it needs.

2.4. Impersonation/Identity Theft

Impersonation is a very common and popular threat among users of networking sites. Impersonators basically make a fake account using the true identity of a person and subsequently use

this account in order to cause issues for the actual identity holder [6] [7] [8].

2.5. Shortened Links

Shortened link/URL is a condensed format of a regular link/URL. It is usually used in twitter where there is a limit of 140 characters for every tweet. However, with the help of shortened URLs' message looks less cluttered. Shortened links have some disadvantages as well. These may lead users to a malicious site which can doubtlessly harm users' system and privacy.

2.6. Surveillance

The omnipresence of social networks also paves the way for unwanted surveillance capability. With the lack of able privacy policies and security protocols, malicious users can invade access user's data both lawfully and unlawfully.

2.7. Psychological Profile Extraction

The data social networks contain generated by their usage by billions of users worldwide, can be accumulated and used to understand how a person thinks and to understand his psychology. That data can help in the extraction of someone's psychological profile which can then be used to understand the user's thinking habits and everything else. This can be an inordinate tool but if used by malicious users, it would be catastrophic.

2.8. Communication Privacy

Users often communicate via social networks and they often share sensitive information in their interactions with each other. Such communications need to be kept safe by any means necessary.

2.9. Security & Privacy worms

Koobface, an example of social network worms, one of the most popular network worm which attacks Microsoft Windows, Mac OSX and Linux systems. Koobface is a network worm that spreads via social networking sites i.e. Facebook, Twitter, Skype, Gmail etc.

This type of worm infects your system and replicates itself via these sites.

3. PRIVACY TECHNIQUES USED FOR ELIMINATING THE ISSUES DISCUSSED ABOVE

3.1. *k*-Anonymity

Latanya Sweeney's K-anonymity was the first known attempt in order to achieve anonymity in networks. In K-Anonymity, attributes are suppressed or generalized until each row is identical with at least k-1 other rows. At this point, the database is said to be k-anonymous. K-Anonymity thus prevents definite database linkages. At worst, the data released narrows down an individual entry to a group of k individuals. Unlike Output Perturbation models, K-Anonymity guarantees that the data released is accurate Suppression and generalization are the methods which are used for achieving K-Anonymity. [9] [8]

- Suppression Method: In this method, attributes of a database can be replaced by a (*). For example, The database in Table 1 transformed into the database in Table 2 after going through suppression at k = 2.
- Generalization Method: In this method, attributes of a database can be replaced with a broader category. For Example, In table 1 the marks: 8.3 can be replaced with Marks: [8.0-8.9].

TABLE 1 - INITIAL DATA

Name	Subject	Course	Marks(CGPA)
Ram	Physics	BBA	8.3
Sham	Mathematics	MBA	7.5
Ram	Chemistry	BA	8.1
Ramesh	Mathematics	MBA	7.5

TABLE 2 - DATA AFTER SUPPRESSION (K=2)

Name	Subject	Course	Marks(CGPA)
Ram	Physics	BBA	8.3
*	Mathematics	MBA	7.5
Ram	Chemistry	BA	8.1
*	Mathematics	MBA	7.5

3.2. l-Diversity

This technique is an extension of K-anonymity. l-diversity helps in preserving privacy in data sets by diminishing the granularity of data representation. l-diversity overcomes the disadvantages (such as homogeneity attack, poor handling of attribute disclosure and background knowledge attack etc.) of K-anonymity model. Basically, l-diversity preserves the different sensitive attributes of the data sets [10].

3.3. *t*-Closeness

t-closeness technique is a further extension of l-diversity. This technique maintains the distribution of sensitive fields. If the distance between the distribution of a sensitive attribute and the whole table attribute is less than or equal to threshold t, then the table is said to have t-closeness [11]. This technique overcomes the limitations of both K-anonymity and l-diversity. The main requirement of t-closeness technique is that the sensitive attribute of both equivalent class and the overall table should be close to each other. Let's assume there are two probabilistic distributions i.e. [11]

$$A = (a1, a2, \ldots . an)$$

and

$$B = (b1, b2, \ldots . bn)$$

, So, the variational distance between them is defined as:

$$\mathrm{D[A, B]} = \sum_{i=1}^{n} \frac{1}{2} |ai - bi|$$

Where:

A = the distribution of the sensitive attribute in equivalent class

B = the distribution of the sensitive attribute in the whole class

3.4. SOKEY (Socially Keyed) Architecture

SOKEY architecture is used to achieve a zero possibility of leakage of sensitive information. There are two requirements needed for designing SOKEY, the first one is 'Zero possibility' and the second one is 'Multilayered nested access control'. The goal of this architecture is to guard the sensitive information in worst cases as well. New key management design and the master key server are used in this architecture. The master key is discovered for the security of the server of social networking sites [12].

4. CONCLUSION

Online Social Networks(OSNs) have become an essential part of everybody's life and like other networks, it has its drawbacks as well. K-anonymity technique aims to prevent the identity disclosure of the users, but it fails in preventing the attribute disclosure of the tables. l-Diversity, being an extended/modified version of K-anonymity, requires at least 'l' values for each sensitive attribute which belongs to that equivalent class. T-closeness technique is a further refined version of l-diversity and overcomes most of the drawbacks of both k-anonymity and l- diversity. T-closeness also succeeds in averting the attribute disclosure of the tables and hence can be established as the best option among the given alternatives.

REFERENCES

[1] L. A. Cutillo, M. Manulis and T. Strufe, "Security and Privacy in Online Social Networks," *Handbook of Social Network Technologies and Applications*, pp. 497-522, 2010.

[2] P. Joshi and C. Kuo, "Security and Privacy in Online Social Networks: A Survey," in *Internation Conference on Multimedia & Expo (ICME 2011)*, 2011.

[3] G. Stringhini, C. Kruegel and G. Vigna, "Detecting Spammers on Social Networks," in *Annual Computer Security Applications Conference (ACSAC)*, 2010.

[4] J. Nagy and P. Pecho, "Social Networks Security," in *Third International Conference on Emerging Security Information, Systems and technologies*, 2009.

[5] T. Jagetic, N. Johnson, M. Jacobsson and F. Menczer, "Social Phishing," *Communications of the ACM*, vol. 50, no. 10, pp. 94-100, 2007.

[6] B. Krishnamurthy and C. E. Wills, "Characterizing privacy in online social networks.," in *Proceedings of the first workshop on Online social networks*, 2008.

[7] G. Wondracek, T. Holz, E. Kirda and C. Kruegel, "A Practical Attack to De-anonymize Social Network Users," in *2010 IEEE Symposium on Security and Privacy*, Berkeley/Oakland, CA, USA, 2010.

[8] L. Lan, H. Jin and Y. Lu, "Personalized Anonymity in Social Networks Data Publication," *IEEE*, 2011.

[9] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy," *International Journal in Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, pp. 557-570, 2002.

[10] A. Machanavajjhala, J. Gehrke, D. Kifer and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," in *Data Engineering, 2006. ICDE'06. Proceedings of the 22nd International Conference on 2006 Apr 3*, 2006.

[11] S. Venkatasubramanian, N. Li and T. Li, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *IEEE 23rd International Conference on Data Engineering*, Istanbul,Turkey, 2007.

[12] J. W. Keister, H. Fujinoki, C. W. Bandy and S. R. Lickenbrock, "Sokey: New Security Architecture for Zero-Possibility Private Information Leak in Social Networking Applications," *IEEE*, 2011.

[13] B. Tripathy and G. Panda, "A New Approach to Manage Security Against Neigborhood Attacks in Social Networks," in *International Conference on Advances in Social Networks Analysis and Mining*, 2010.

[14] A. Kumar, S. K. Gupta, S. Sinha and A. K. Rai, "Social Networking Sites and Their Security Issues," *International Journal of Scientific and Research Publications*, vol. 3, no. 4, April 2013.

[15] K. B. Kansara and N. M. Shekokar, "Security against sybil attack in social network," in *International Conference on Information Communication and Embedded System*, 2016.