International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 06 | Sep-2015 www.irjet.net p-ISSN: 2395-0072

SURVEY PAPER ON MOBILE SOCIAL NETWORKS

A. Vijaya Lakshmi [1], Dr. S. Britto Ramesh Kumar [2], P. Joseph Charles [3]

[1] Research Scholar, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India
[2] Assistant Professor, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India
[3] Assistant Professor, Department of Information Technology, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India

---

Abstract *- **Social Networks (SN) Sites are becoming very popular and the number of users is increasing rapidly. A typical MSN provides each user with a virtual space containing profile information, a list of the user's friends, plus web pages, such as wall in Face book, where users and friends can post content and send messages. A user profile usually includes information with respect to the user's birthday, gender, interests, education and employment history, and contact information. Although MSNs currently provide simple access control mechanisms allowing users to govern access to information contained in users own spaces, they unfortunately, have no control over data residing outside their spaces. For example, Face allows users to state who is allowed to insert messages in their walls.***

Key Words: *Social Networks, Mobile Social Networks, Security, Privacy*

1. INTRODUCTION

A social networking service is a platform to build social networks or social relations among people who, for example, share interests, activities, backgrounds, or real-life connections. A social network service consists of a representation of each user (often a profile), his/her social links, and a variety of additional services. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered.

2. LITERATURE REVIEW

Aaron et al. [1] proposed Secure Social Aware: A Security Framework for Mobile Social Networking Applications in which he presented a framework called SSA, it allows for the interaction of social network information with real-world location-based services without compromising user privacy and security. Through exchanging an encrypted nonce (EID) associated with a verified user location, SSA allows location based services to query the local area for social network information without disclosing user identity or any set of information which could be positively matched to users.

Yan et al. [2] have proposed a Collaborative Framework for Privacy Protection in Online Social Networks. System architecture for a private OSN is proposed to protect privacy. The main task of cryptography in building a private OSN is to restrict the information available in an appropriate range. Users make use of relationships or social links to represent this range in a social network. Anna et al. proposed PriMa, an effective security and privacy protection mechanism for social networks. PriMa (Privacy Manager) automatically generates access rules for users profile information.

In this attack, the adversary first tries to find ways to obtain victim's personal information, such as name, location, occupation and friends list from his public profile on OSNs or his personal homepage(s). Online Social Network Services (OSNs) are today one of the most popular interactive medium for communicating, sharing, and disseminating a considerable amount of human existence information. Daily and continuous communications imply the exchange of several type of content, including free text, picture, audio, and video data. However, OSNs face a large number of attacks which affects the privacy and security of its users. In this section, I will discuss the various attacks in OSNs. For instance, if users post a comment in a friend's space, they cannot specify which user can see the comment. In another case, when a user uploads a photo and tags friends who appear within the photo, the tagged friends cannot restrict who can see this photo. Spammers are always looking for ways to reach new victims with their unsolicited messages.

In a social network, the first action a malicious user would likely execute to get in touch with his victims is to send them a friend request. This might be done to attract the user to the spammer‟s profile to view the spam messages (on MySpace) or to invite user to accept the friendship and start seeing the spammers messages in her own feed. In Web, most identity management system models such as silo model, centralized model, and

federated model are designed from organizations perspective. The posted content can be re-distributed by the viewers, and eventually the content can be shared with unintended users who were not explicitly allowed to view that content. Such open sharing availability of social networking sites exposes the users to a number of privacy risks.

The primary goal of EASiER is to protect accidental or intentional information leak in OSN through encryption, specifically ABE, chosen for its expressiveness. Unlike traditional OSNs, which generally support one type of relationship such as friend, EASiER users define relationships by assigning attributes and keys to each other. To protect information, users encrypt different pieces of data such as profile information, wall posts, etc. with attribute policies. Thus OSNs are suffered by various security and privacy attack. In this paper, I propose an idea to overcome the issues with content preference and security policies.

Anna et al. [3] proposed PriMa, an effective security and privacy protection mechanism for social networks. PriMa (Privacy Manager) automatically generates access rules for users profile information. PriMa access rules are generated on the basis of users' privacy preferences on their profile data, the sensitivity of the data with respect to the privacy settings of the user such as his privacy preferences for his profile data and the degree to which his profile data is at a risk of being exposed to others, and the risk of disclosing such data to other users. These access rules allow users to enforce fine-grained protection, such that the rules can be stated for different levels of granularity ranging from single traits to an entire class of them. Due to this fine grained control, accidental disclosures are avoided. Hence, PriMa reduces the chance of accidental disclosures due to outdated policies. However, there still exist many shortcomings to be overcome before PriMa can be regarded to be completely sufficient in protecting the user's information.

Hongxin et al. [4] have proposed a novel solution for Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks. A systematic conflict detection and resolution mechanism is addressed to cope with privacy conflicts occurring in collaborative management of data sharing in OSNs. Conflict resolution approach balances the need for privacy protection and the users desire for information sharing by quantitative analysis of privacy risk and sharing loss.

Philip et al. [5] devised a model for Preventing Sybil Attacks by Privilege Attenuation for Social Network Services. A static policy analysis for verifying if an Facebook-style Social Network Services(FSNSs) is Principle of Privilege Attenuation (POPA) compliant. To prevent unprivileged users from colluding with one another to gain access, Denning advocates the Principle of Privilege Attenuation (POPA). Denning's Principle of Privilege.

Attenuation (POPA) is formalized as a run-time property, and demonstrated as a necessary. It is a sufficient condition for preventing the Sybil attacks. To prevent Sybil attacks, a group of unprivileged users cannot collude to gain privilege. That is, the establishment of privilege requires the cooperation of at least one privileged user. In the following, it is demonstrated that the two conditions are in fact equivalent, and thus POPA compliance is not only sufficient but also necessary for preventing Sybil attacks. First, this work studies Sybil attacks in the novel context of a Relationship-Based Access Control system (i.e., FSNSs), rather than peer-to-peer or recommendation systems. However, the results in this work apply only to monotonic policies. And also the challenge will be to minimize the runtime and storage overhead required for such a scheme. The following Figure1 represents the nodes between accessor and owner.

Gilbert et al. [6] introduced a Practical Attack to DeAnonymize Social Network Users, that exploits group membership information that is available on social networking sites. There exists some kind of hierarchy within a group. That is, particular members can hold the role of administrators or moderators, which grants them some special privileges. To determine the group membership of a user, web browser history stealing attacks is used. Thus, whenever a social network user visits a malicious website, this website can launch deanonymization attack and learn the identity of its visitors. The information about the group memberships of a user is sufficient to uniquely identify the user.

Lujun et al. [7] introduced security and privacy wizards for social networking sites. The goal of the Wizard is to automatically configure a user's privacy settings with minimal effort from the user. Ideally, the wizard should satisfy the following requirements: Low Effort, High Accuracy. A generic framework is developed for the design of a privacy wizard. . This type of interaction is ideal for non-technical users, who have difficulty reasoning holistically about their policy configurations.

Hassan et al. [8] have proposed a process towards active detection of identity clone attacks on online social networks. A new attack called Identity Cloning Attack (ICA), which focuses on forging user profiles on OSNs, has been introduced. In this attack, the adversary first tries to find ways to obtain a victim's personal information, such as name, location, occupation and friends list from his public profile on OSNs or his personal homepage(s).

Comparative analysis

Author	Proposed work	Advantages	Drawbacks/Limitation	External device
Hongxin Hu	Enable collaborative privacy management of shared data in OSNs.	system evaluation and usability study	Security and privacy challenges	NO
Marco Vanetti	OSN users to have a direct control on the messages posted on their walls.	Automatically labeling messages in support of content-based filtering.	Message is blocked	No
Aaron Beach	Secure Social Aware (SSA) which allows for the interaction of social network information with real-world location-based services without compromising user privacy and security.	User security	set of social network information associated with a set of users is chosen such that the set of preferences can-not map back to any one or any set of the users within some guarantee	No
Yan Zhu,	Collaborative framework which enforces access control for OSN through an innovative key management focused on communities.	privacy management approaches for OSN leverages a key management technique to enable a user to simply post encrypted contents so that only users who can satisfy the associate security policy can derive the key to access the data	Less Security	No
Anna Squicciarini	privacy protection mechanism which supports semi-automated generation of access rules for users' profile information.	The resulting rules are simple, yet powerful specifications	Semi-automated generation of access rules for users' profile information.	No

Lei Jin,Hassan	Detection framework that is focused on discovering suspicious identities and then validating them.	to demonstrate flexibility and effectiveness of the proposed approaches	The limitations and develop a Facebook or Linkedin third-party application to implement they proposed detection schemes in a more real OSN environment	No
Leyla Bilge	the automated identity theft of existing user profiles and sending of friend requests to the contacts of the cloned victim.	effective and feasible to launch an automated, cross-site profile cloning attack.	Less user network	NO
Markus Huber	novel friend injection attack which exploits the fact that the great majority of social networking sites fail to protect the communication between its users and their services	protect the communication between its users and their services	fail to protect their users against malicious eavesdroppers and injection attack	No

3. CONCLUSION

Social network sites are a major application driver with millions of users all over the world relying on them in keeping contacts and sharing information with others. This huge involvement drives the need for setting the right security measures that help in protecting users' privacy. The vulnerabilities of this method have been well known for attackers to guess, because the users often create memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember.

REFERENCES

[1]. Aaron Beach, Mike Gartrell, Baishakhi Ray, Richard Han, "Secure Social Aware: A Security Framework for Mobile Social Networking Applications", in Proc. IEEE International Conf. on 2012, pp. 439-446.
[2]. Yan Zhu, Zexing Hu, Huaixi Wang, Hongxin Hu, Gail-Joon Ahn, "A Collaborative Framework for Privacy Protection in Online Social Networks", in Proc. 6th Annu. IEEE International Conf. on 2010, pp. 1 – 10.
[3]. Anna Squicciarini, Federica Paci, Smitha Sundareswaran, "PriMa: An Effective Privacy Protection Mechanism for Social Networks", in Proc. of IEEE 3rd International Conf. on 2011.
[4]. Hongxin Hu, Gail-Joon Ahn and Jan Jorgensen, " Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks", in Proc. of ACM International *conf. on* 2007, Vol.4, Issue 8, pp.538-542
[5]. Philip W. L. Fong, "Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems", in Proc. of IEEE International Conf. on 2008.
[6]. Gilbert Wondracek, Thorsten Holz, Engin Kirda, Christopher Kruegel, "A Practical Attack to De-Anonymize Social Network Users", in Proc. Of IEEE, 2011.
[7]. Lujun Fang and Kristen LeFevre, "Privacy Wizards for Social Networking Sites", in Proceeding of IEEE 3rd International conf. on 2011.
[8]. Lei Jin, Hassan Takabi, James B.D. Joshi, "Towards Active Detection of Identity Clone Attacks on Online Social Networks," in Proc. ECDC of 7th International Conf. on 2013, pp. 1- 12.

AUTHOR'S BIOGRAPHY

A. Vijaya Lakshmi received her Master's in Computer Science from Bharathidasan University, Tiruchirappalli, India. Currently, she is a M.Phil Scholar in the department of Computer Science, St. Joseph's College, Tiruchirappalli affiliated to Bharathidasan University, India. Her main area of research is Security in Mobile Social Networks. She has presented two papers in the National Conference. She has atteneded several national and international conferences and workshops.

Dr. S. Britto Ramesh Kumar is an assistant professor of Computer Science at St. Joseph's College (Autonomous), Tiruchirappalli. His research interests include software architecture, wireless and mobile technologies, information security and Web Services. He has published many journal articles and book chapters on the topics of Mobile payment and Data structure and algorithms. His work has been published in the International journals and conference proceedings, like JNIT, IJIPM, IEEE, ACM, Springer and Journal of Algorithms and Computational Technology, UK. He awarded as a best researcher for the year 2008 at Bishop Heber College, Tiruchirappalli. He guides 8 Ph.D. research scholars and has completed a minor research project. He visited the countries like China, South Korea and Singapore.

P. Joseph Charles is currently works as an assistant professor in department of information technology, St. Joseph's College (Autonomous), Tiruchirappalli. His areas of interest include context aware web services, information retrieved, etc. He has published nearly twenty research papers in international and national journals. Among three papers were scopes indexed.