ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

SOCIAL NETWORK SERVICES: AN OVERVIEW

S.Thiraviya Regina Rajam[1] and Dr. S.Britto.Ramesh Kumar[2]

Research Scholar, St. Joseph's College (Autonomous), Tiruchirappalli[1]

Assistant Professor in Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli[2]

Abstract: The past few years a tremendous growth on Online Social Networks such a Facebook, Orkut and Twitter is seen. These OSNs not only offer attractive means for virtual social interactions and data sharing, but also raise a number of security issues. Although OSNs allow a single user to access to her or his data, they currently do not provide any mechanism to enforce privacy protection over data associated with large number of users, leaving privacy violations largely unresolved and leading to the potential disclosure of information that at least one user intended to keep private. This paper analyses the various privacy and security issues in OSNs. OSNs come across various types of attacks such a fake identity, Sybil attacks, Identity clone attacks, The main aim is to enhance the privacy and security in OSNs which is one of the Quality of Service (QoS) issues and thereby decreasing the attacks and issues. This paper is a survey which is more specific to expose the various attacks and privacy models in OSNs with respect to enhancement of security and privacy.

Keywords: Security, privacy, Sybil attacks, Identity Cloning attacks, Quality of Service (QoS).

1. INTRODUCTION

A variety of social networking sites (SNSs) are used by hundreds of million users. At the time of writing Facebook is the biggest online social networking service with over 400 million active users. Users provide personal information about themselves including their interests, social relationships, current occupation, pictures and other media content, and share this information via SNSs platforms. Due to the sensitivity of information stored within social networking sites a variety of research in the area of information security has been conducted. While there is a continual flow of media stories discussing privacy and security problems of SNSs, the great majority of academic contributions focus either exclusively on\ possible threats on one hand, or possible protection strategies on the other. However, there are various privacy and security issues in OSNs. Although OSNs currently provide simple access control mechanisms allowing users to govern access to information contained in own spaces, users, unfortunately, have no control over data residing outside their spaces. For example, Facebook allows tagged users to remove the tags linked to their profiles or report violations asking Facebook managers to remove the contents that they do not want to share among the public.

However, these simple protection mechanisms suffer from a number of limitations. On one hand, removing a tag from a photo can only prevent other members from seeing a user's profile by means of the connection link, but the user's image is still contained within the photo. Since original access control policies remain unchangeable, the user's image continues to be revealed to all approved users. Social networking sites have been studied in a variety of academic disciplines. Scholars from social sciences have studied impact SNSs have upon the young generation and their motives to join online social networks [1], [2], [3], [4]. To defend user data, access control has become a central feature of OSNs [5], [6]. Recent studies [7] have shown that the user interaction graph is much less dense than friendship graph, indicating that users interact most frequently with a small group of friends, further validating the need for fine-grained access control. The main contributions of this paper are:

- Summary of issues in OSNs.
- Summary of Security required to avoid various attacks in OSNs.
- Summary of related papers.

Section 2 provides an overview of issues on Social Networking services, Section 3 contains Security Requirements, Section 4 focus on Background-Related works, we conclude on Section 5, Section 6 discuss about the Future Enhancements along with References.

2. ISSUES ON SOCIAL NETWORKING SERVICES

Internet is considered to be the foundation for Social Networking Sites. Social Networking sites are used by a large number of users all over the world. It provides various features to the customers like chating, posting comments, Video chating etc. However, it is affected by various attacks which affects the customer's privacy and security. Some of the issues on Social Networking Services are: 1. DIGITAL DOSSIER AGGREGATION - SNS profiles can be fetched and stored by third parties in order to create a digital dossier

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

of personal data[8]. 2. CBIR (CONTENT-BASED IMAGE RETRIEVAL) - CBIR is a technology which deduces the location of users by analyzing and comparing common pattern in images. Hence shared images within SNSs not only disclose the identity of users but possibly the location of users as well. 3. SECONDARY DATA COLLECTION VULNERABILITIES – SNS members also disclose information to their Internet service providers (ISPs). While this is not solely limited to SNSs, the main difference is the extent of coherent personal data exposed to ISPs [10]. 4. LINKABILITY FROM IMAGE METADATA, TAGGING AND CROSS-PROFILE IMAGES - While users control which information and media they share inside a SNS, they can't control which content other users upload and link to their own profile. Images might also contain metadata including the serial number of the camera used to make the pictures. 5. DIFFICULTY OF COMPLETE ACCOUNT DELETION – Users that wish to deactivate their SNS account face difficulties to do so in most cases [9]. On the one hand because not all comments and messages sent to other users are deleted, and on the other hand because SNS providers keep backups of account data. 6. SOCIAL NETWORKING SPAM - As SNSs steadily grow they have become interesting targets for spammers. The use of SNS spamming software furthermore automates the process of sending unsolicited mass messages.

The Spam content can reach from advertising to Phishing messages. 7. CROSS SITE SCRIPTING, VIRUSES AND WORMS - In order that users are able to customize the design of own profiles, SNSs often provide the possibility to post HTML code. Furthermore third party applications are used to extend the functionality of SNSs and together with HTML code they state a risk for Cross-site scripting vulnerabilities [11]. 8. SNS AGGREGATORS - Social Aggregators offer services to integrate the data from different web services and SNSs into a single platform. Popular services include Gathera, FriendFeed, Spokeo and Secondbrain [13]. As with all single-sign-on systems, the access to multiple services (in this case SNSs) depends on only one password which if selected badly states a single point failure.

These services are also used to correlate user data across different SNSs. 9. SPEAR PHISHING USING SNSS AND SN-SPECIFIC PHISHING - Spear Phishing attacks [12] are targeted Phishing attacks. The information available through SNSs is harvested by scammers and used as a basis for a spear Phishing attack. 10. INFILTRATION OF NETWORKS LEADING TO INFORMATION LEAKAGE - SNSs allow users to define who has access to their personal information, for example by giving access to certain "friends" or by defining restricted groups (networks). These are important features to improve the privacy issues of SNSs usage but once a closed network is infiltrated the protection is rendered useless. These are some of the issues in Social Networking Sites.

3. SECURITY REQUIREMENTS

Since there is a large number of security issues, OSNs need security mechanisms for the security and privacy of users. The various security requirements needed for users are described below. Recently various data protection schemes have been proposed to protect the user's privacy in social networks against malicious or curious entities. These entities might either be the social network operator itself, someone from within the users' social context, or an external adversary who tries to use social networks as attack vector. Common methods for defense include the use of encryption, data dissociation or the usage of fake information. A combination of these methods is likely to protect the users' privacy to a larger extend. Encryption can be used to secure communication channels. In the most naive approach this means that the communication between the users and the social network uses encryption (e.g., HTTPS) [14] to protect against eavesdropping. Stenography might be used to embed information in pictures or videos hosted or exchanged over SNS. As the videos and pictures are transformed upon submission to fit the size constraint of the websites, the steganographic algorithms [15] need to be robust enough to withstand these transformations. Fake identities require major security issues. It is quite common that several people have similar names in real world; and hence their identities on OSNs may be similar.

It is not possible to arbitrarily infer all the similar identities that have similar names as faked identities. Data dissociation can be used to separate the amount of data stored at the SNS. All publicly available information can be stored at the SNS, while private and sensitive information could be stored at a third party e.g., the computer of the user, a trusted third party, or an un trusted third party. To protect the information at the un trusted third party, encryption can be used to allow confidentiality or fine grained access controls [16]. Fake information can be used as an additional layer of protection against curious social networking operators or external adversaries. The social network only sees the fake information, while possibly authentic and sensitive information is stored encrypted on a third party server. As a source for fake information either predefined wordlists or dynamic content from the Internet might be used. However, Security should be mainly focused on content preference, Tagging photos, anonymous friend requests and Authentication should be provided for users whenever h/she is logging in to their own account.

4. RELATED WORKS

This section presents the background information about the various works on security and privacy issues in OSNs. In this Section we shall discuss on the existing failure prediction, detection and correction methods for OSN security and privacy. Failure prediction determines the possible occurrences of fatal events in the future. Existing

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

methods provides security to the customers. However, there are some draw backs which affects the user from getting full security. The various related works on OSNs are discussed below.

***A*nna et al. (2011)** proposed PriMa, an effective security and privacy protection mechanism for social networks [17]. 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.

***H*ongxin et al. (2012)** have proposed a novel solution for Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks [18]. 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. A collaborative privacy management mechanism for the protection of shared data with respect to multiple controllers in OSNs is addressed. Privacy Conflict Identification can be done through specifying the privacy policies to reflect the privacy concern. Each controller of the shared data item defines a set of trusted users who can access the data item**.** Identification of Conflicting Accessor Space Algorithm is used in privacy conflict identifications. Privacy Conflict Resolution is the process in which it makes a decision to allow or deny the accessors within the conflicting segments to access the shared data item. However, the privacy risk of a conflicting segment is an indicator of potential threat to the privacy of controllers in terms of the shared data item. The higher the privacy risk of a conflicting segment, the higher the threat to controllers' privacy**.**

***P*hilip et al. (2011)** devised a model for Preventing Sybil Attacks by Privilege Attenuation for Social Network Services [19]. A static policy analysis for verifying if an Facebook-style Social Network Services(FSNSs) is **P**rinciple **o**f **P**rivilege **A**ttenuation (POPA) compliant. To prevent unprivileged users from colluding with one another to gain access, Denning advocates the **P**rinciple **o**f **P**rivilege **A**ttenuation (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 run-time and storage overhead required for such a scheme. The following Figure1 represents the nodes between accessor and owner.

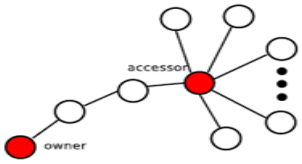

Figure 1: Nodes between Accessor and Owner

***G*ilbert et al. (2010)** introduced a Practical Attack to De-Anonymize Social Network Users [20], 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 de-anonymization attack and learn the identity of its visitors. The information about the group memberships of a user is sufficient to uniquely identify the user.When unique identification is not possible, then the attack might still significantly reduce the size of the set of candidates that the victim belongs to. However, this attack requires a low effort, and has the potential to affect millions of registered social networking users who have group memberships and also many more social networks that support group memberships can potentially be misused for similar attacks.

***L*ujun et al. (2012)** introduced security and privacy wizards for social networking sites [21]. 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. The basic

structure of a binary decision tree is easily interpretable: Each interior node represents a binary condition (e.g., Hometown = NYC), and each leaf contains a decision (allow or deny). Each node (either interior or leaf) corresponds to a set of friends that are consistent with the binary conditions from root to the node. we incorporate two additional pieces of information for each node. This model, then, is used to automatically configure the user's detailed privacy settings. However, even if the site hides users political affliation, it may still be possible for an attacker to infer the hidden information.

***H*assan et al. (2013)** have proposed a process towards active detection of identity clone attacks on online social networks [22]. 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). Then, the adversary forges the victim's identity and creates a similar or even identical profile on OSN sites. Afterwards, he sends friend requests to the victim's contacts. Once the friend requests are accepted, he builds the victim's friend network and gains access to profiles of the victim's friends. In addition, he can launch ICAs on the victim's friends based on these personal data. In our detection process, a flexible set of parameters is used, which can be adjusted to distinguish a victim from its clones and may achieve accurate detections on different OSNs where the faked identities may have different behaviors. The first attempt to characterize the faked identities, and detect them on OSN sites using an active approach based on profile similarity. Second, two profile similarity schemes is proposed to discover suspicious identities. However, Some individuals never use the social network systems. When adversaries get enough personal information of these individuals, they can create faked identities without any misgiving to forge them and deceive their friends.

CONCLUSION

A number of practical attacks have been outlined by researchers in the last five years and a fast number of actual attacks have been observed in-the-wild. Given the emerging threats of social networking usage we hence explored mitigation strategies for these attacks. As the penetration of the social networks in our lives increases, we may see abuses as well as the benefits of the technology in future. In this paper we have tried to present an overview of social networks with the various techniques used in the analysis of social network Services (OSNs). We have also tried to discuss the challenges and the emerging research areas associated with the analysis of Social Networks. OSNs has its own merits and demerits. In this paper we have discussed the various issues in OSNs and we have also reviewed various papers which focuses on the security and privacy of OSNs. The study shows that there are various new privacy and security mechanisms that are available and also discusses about the drawbacks in the reviewed papers. These issues should be rectified in order to provide secure OSNs for users.

REFERENCES

1. D. Boyd., " Social Network Sites: The Role of Networked Publics. Teenage Social Life. Youth, Identity and Digital Media". 2007, pp 119–142.
2. D.M. Boyd and N.B. Ellison, " Social network sites: Definition, history, and scholarship", International journal of computer mediated communication-electronic edition, 2007..
3. C. Dwyer. "Digital relationships in the Myspace generation: Results from a qualitative study," in Proc. of 40th Annu HICSS International Conf. on 2007, pp. 19–21..
4. S. Livingstone, "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self expression," 2008, pp. 388-393.
5. L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda," All your contacts are belong to us: automated identity theft attacks on social networks," in Proc. of 18th ACM International Conf. 2009, pp. 551–560.
6. B. Carminati, E. Ferrari, and A. Perego, " Enforcing access control in web-based social networks," in Proc. ACM Transactions on Information and System Security (TISSEC), 2009, 13(1):1–38.
7. A. Mislove, M. Marcon, K. P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in Proc. of IMC, 2007.
8. R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: An online social network with user-defined privacy," in Proc. ACM SIGCOMM Computer Communication Review,2009, pp.135–146.
9. M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, and C. Kruegel, "Abusing Social Networks for Automated User Profiling," 2010.
10. BBC News. Jail for Facebook spoof Moroccan. online, 2008. [Retrieved 2008-12-01].
11. Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda, "All your contacts are belong to us: Automated identity theft attacks on social networks," in Proc. 18th International World Wide Web Conf. on 2009.
12. J. Bonneau, "Security and Privacy in Social Networks," online [Retrieved 2010-05-10].
13. J. Bonneau, J. Anderson, R. Anderson, and F. Stajano, "Eight friends are enough: social graph approximation via public listings," In Proc. of the 2nd ACM EuroSys Workshop on Social Network Systems, 2009,pp. 13–18.
14. W. Luo, Q. Xie, and U. Hengartner,"FaceCloak: An Architecture for User Privacy on Social Networking Sites," in Proc. of CSE International Conf. on 2009.
15. http://blog.trendmicro.com/ new-variant-of-koobface-worm-spreading-on-facebook/[Online: accessed 14-March-2010].
16. A. Mislove, M. Marcon, K.P. Gummadi, P. Druschel, and B. Bhattacharjee, "Measurement and analysis of online social networks," in Proc. of the 7th ACM SIGCOMM International Conf. on 2007, pp. 42-45.
17. Anna Squicciarini, Federica Paci, Smitha Sundareswaran, "PriMa: An Effective Privacy Protection Mechanism for Social Networks," in Proc. of IEEE 3rd International Conf. on 2011.
18. 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.
19. 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.
20. Gilbert Wondracek,Thorsten Holz,Engin Kirda,Christopher Kruegel, "A Practical Attack to De-Anonymize Social Network Users,"in Proc. of IEEE, 2011.
21. Lujun Fang and Kristen LeFevre,"Privacy Wizards for Social Networking Sites," in Proc. of IEEE 3rd International conf. on 2011. 22. 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.