An Analysis on Online Social Network Security

Shailendra Rathore, Saurabh Singh, Seo Yeon Moon, Jong Hyuk Park*
Dept. of Computer Science and Engineering, Seoul National University of Science and Technology (SeoulTech),
Seoul, 139-743, REPUBLIC OF KOREA
E-mail: {rathoreshailendra, singh1989, moon.sy0621, jhpark1}@seoultech.ac.kr

Abstract

Online social networking sites such as MySpace, Facebook, Twitter are becoming very preeminent, and the quantities of their users are escalating very quickly. Due to the significant escalation of security vulnerabilities in social networks, user's confidentiality, authenticity,and privacy have been affected too. In this paper, a short study of online social network attacks is presented in order to identify the problems and impact of the attacks on World Wide Web (WWW).

1. Introduction

An Online Social Network (OSN) is a type of website to develop virtual social networks between people with the same point of interests, activities, backgrounds or people that know each other from the real life [1].These networks allow users to find new friends and develop their friend circle. Moreover, sharing is another important feature of OSN. Users can share their photos, videos, activities, interests and many more items. In recent years, the use of OSN has rapidly grown. Some OSN for instance, LinkedIn, Facebook and MySpace have been very famous and become the preferred way of communication for many people. The significance of these websites comes from the fact that the users spend a high amount of time to update their information, interact with other users and surf other members' profiles. OSN can be very beneficial for the users because it eliminates the geographical and economical borders. In addition, OSN can be utilized for achieving the targeted goals such as educational, entertainment, job searching and much more. However, this popularity of OSN acts as a high risk to OSN users. A significant amount of data that the users store on OSN make the OSN a desirable target for adversaries. Adversaries can obtain sensitive personal data simply by using OSN [2, 3]. Moreover, as a result of the high amount of user's activities, personal data that is shared on these networks are up-to-date. Therefore, users are inspired to supply personal data such as name,

interests, and date of birth, gender, address, educational information, place of birth, and other sensitive information in OSN sites. This data can be shared with other OSN users. Later, adversaries can detect other significant data by analyzing this data. The more data users upload, the more data an adversary will gain.

According to Sophos Security Threat Report- 2011 [4], 0.5 billion online users on the web use Facebook. This report reveals that Facebook is under the biggest security risk, significantly ahead of MySpace, Twitter and LinkedIn as shown in Figure 1. It is a most popular destination of active users on the web. Due to this popularity, a lot of users are intensely attacked by adversaries with various type of attacks such as malware, phishing, spamming, etc. These attacks are proliferating continually.

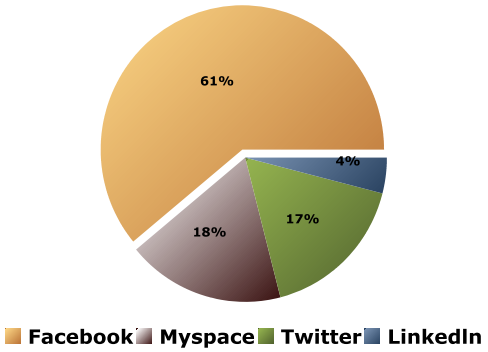

Fig. 1: Sophos security threat report- 2011 [4]

2. OSN Security problem and impact

Some significant features of OSN such as sharing pictures, commenting, tagging, and blogging have turned it into the part of the daily lifecycle for billions of web users. Though consequently, OSN users reveal themselves to several kind of privacy problems, which we will discuss in the following sections.

Safety related problem: As a result of the huge volume of private user data available on OSN, users might be easily revealed to internet threats such as identity theft, spear phishing, online fraud, online predator and other cybercriminal attacks. As reported by Symantec's web Security document-2008 [5], OSN has turned into a most promising target of the attacker for the identity theft attack.

Reputation related problem: Reputation is a type of common assessment of the community towards an individual, an association or a group of people. It plays a vital role in many areas such as corporate, social status, online groups [6]. As several people rely on OSN for recording their life and for keeping in touch with their friends. Moreover, OSN can be used for passing their statements and images beyond their friend's circle. With this high utilization of OSN, online reputation of users are also accelerated over the web. Subsequently, reputations of the user also influences user status and credibility in real-life.

Profiling problem: According to a definition from Electronic Privacy Information Center (EPIC) [7], profiling is a procedure for making chronicle and for categorization of behaviors. Several companies gather data from a variety of third party resources (such as OSN) for making profile of individuals and their behavior with the intention of selling products to them. This is typically accomplished without the individual's permission.

3. Taxonomy of OSN attacks

OSN is described as an interactive internet-based application that enables users to communicate with their friends and family, meeting with new users, organize events, conversations, posting photos/videos and links with new people in the same way as in real life. The sensitive information is shared on OSN, makes it more vulnerable for launching cyber-attacks by adversaries. A continuous escalation of exchanged information also escalates the information leakage risks [8]. There are different type of attacks on OSN. In this section, a taxonomy of OSN attacks is described. The different type of attacks on OSN are as follow.

Identity-based attacks: Identity theft is a type of threat in which adversary steal the identity or confidential information of a person and later, pretend to be that person, or using that confidential information or identity in a wrong manner. OSN is a most promising target of adversary for identity theft. Since, it contains a high amount of available user's information. Typically, OSN users submit their unique e-mail address and provide sensitive information such as their contacts, current relationship, date of birth, activities in which they involve, and information about his professional and education background, etc. Therefore, from the view of adversaries, they can access this kind of detailed information and can launch attacks such as social engineering, spear phishing, Sybil attack, and Profile-Squatting.

Social relationship -based attacks: In this type of attack, adversaries take advantage of social relationship on OSN. These include Cyber-bullying and grooming, Corporate Espionage and Stalking. Cyber-bullying is a repetitive harassing or harming through the internet in a deliberate way while in the cyber-grooming, adults try to establish an emotional connection with children through the web for abusing them sexually. Typically, minor is an appropriate susceptible age-period for the internet attacks. The persons under this age easily become the target of cyber bullying attack and are highly targeted by online predators. Moreover, a corporate espionage can perform automated social engineering attack using OSN. In stalking, OSN users frequently

reveal location-based information through their images (Content-based Retrieval)[9].

Information security attacks: These type of attacks involve Spamming, Malware, Phishing, and Cross Site Scripting (XSS). In spamming attack, adversaries send advertised messages in a bulk amount to the internet users. The spamming attack through OSN is appeared to be more successful in comparison with the traditional spamming attack in which email is used for spreading spams. This spreading of spam is because of the social relationship between users. In addition to spamming, malware is a kind of malicious program that consists of Trojan horses, viruses, and worms. Generally, OSN websites work upon connections of different user's system. Therefore, malware can simply transfer over these connections between the various user's systems. Another traditional information security attacks in OSN are Cross-site Scripting (XSS) and phishing attack. The XSS attack is due to third party applications with malicious HTML codes, while in phishing, adversaries use fake websites and emails to reveal user's sensitive private information.

4. Conclusion

OSNs can be an efficient and fun service for a user to share his interest and engage with his friends without geographical and economical limitations. In the same time, these networks can put the user at a serious cyber security risk. In this paper, we have studied most common attacks on OSN and discussed, how each of these attacks might put the user in danger.

Acknowledge

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government (MSIP) (No. 2016R1A2B4011069).

References

[1] Helena Bilandzic, Geoffroy Patriarche, and Paul J. Traudt, *The social use of media: cultural and social scientific perspectives on audience research*, Intellect Books, 2012

[2] NEXGATE, "Research Report 2013 State of Social Media Spam," http://nexgate.com/wp-content/uploads/2013/09/Nexgate-2013-State-of-Social-Media-Spam-Research-Report.pdf

[3] "We are social "Digital, Social & Mobile Worldwide in 2015," http://wearesocial.com/uk/special-reports/digital-social-mobile-worldwide-2015

[4] "Sophos Security Threat Report- 2011," https://tavaana.org/sites/default/files/sophos-security-threat-report-2011.pdf

[5] Symantec, "Cybercrime gets personal: Social networking sites next top targets for identity theft 2008." http://www.symantec.com/en/uk/about/news/release/article.jsp?prid=20080420_01, Access online August 2016

[6] Luca Maria Aiello, Martina Deplano, Rossano Schifanella, and Giancarlo Ruffo. "People are Strange when you're a Stranger: Impact and Influence of Bots on Social Networks, " arXiv preprint arXiv: 1407.8134, 2014

[7] "Electronic Privacy Information Center (EPIC)." https://www.epic.org/. Access online August 2016.

[8] Natarajan Venkatachalam, and R. Anitha. "A multi-feature approach to detect Stegobot: a covert multimedia social network botnet," Multimedia Tools and Applications, pp. 1-18, 2016

[9] Varun Kacholia, Ashutosh Garg, and David Stoutamire. "Spam detection for user-generated multimedia items based on concept clustering," U.S. Patent No. 9,208,157, 8 Dec. 2015