Defusing the Hazards of Social Network Services
SeyedHossein Mohtasebi and Ali Dehghantanha
Asia Paci_c University College of Technology and Innovation,
Kuala Lumpur, Malaysia
fshmohtasebi,dehqang@gmail.com

ABSTRACT

Over the past few years, hundreds of millions of users have employed social network services (SNS) to exchange information. In spite of the pros of using SNS, there are certain vulnerabilities that are most likely to be exploited by perpetrators to reach their destructive goals.
Due to an immense amount of personal data shared on and transmitted over SNSs and weak protection mechanisms, the uploaded information are vastly vulnerable to privacy intrusion threats. Furthermore, nearly all SNSs provide a variety of communication channels which opens more ways to malwares to infect users' machines. This paper encompasses threats, vulnerabilities, and risks that endanger privacy of SNS users. It also investigates techniques used by cybercriminals for propagating malicious software (malware) and launching attacks against victims' machines through these services. The paper eventually presents a set of recommendations to eliminate or mitigate the privacy and malware risks of SNS.

Keywords: Social network service; privacy; malware;

1 Introduction

In recent years, the number of SNS users has spectacularly increased. Only Facebook as one of the dominant SNSs has over 750 million active users in which each of which, in average, is linked to 130 other users and facebook.com is the second most visited website on the Internet [1, 2]. Events happened across the Middle East and North Africa in early 2011 that many of them were organized by SNSs are evident in the importance and e_ectiveness of social networks [3-5]. Nonethe-less there have been always privacy and secrecy concerns regarding abusing the uploaded information by Internet perpetrators like cyber-stalkers and even ad- versaries who employ SNSs for reconnaissance purposes before start attacking an organization. Additionally, SNS is a perfect platform for virus authors to spread their malwares faster than traditional methods since the structure of social net-works is the combination of almost all long-established Internet communications channels such as email and instant messaging (IM).
Furthermore, some SNSs enable developers to share their applications and as a result, it facilitates dis-tributing malwares that are covered in the form of a useful application. The main contributions of this paper are to propose felicitous methods for miti-gating the vulnerabilities and consequently circumventing the privacy and mal-wares threats of SNS. The remainder of this paper proceeds as follows: Section 2 studies the potential dangers regarding privacy issues within SNS. It also delves into the functionality of malwares that by using SNS propagate themselves or
launch attack against third parties’ machines. Section 3 offers a holistic approach to reduction the security risks that are caused by the identified threats. The last section, finally, concludes the work and discusses highlights work.

2 State of the Art
In order to eradicate or at least lessen the risks, it is imperative to identify threats that could exploit the vulnerabilities of SNS. Current SNSs are facing myriad threats; this work is, however, mainly concentrating on privacy breach and malware infection. This section is intended to review the current situation of the privacy and malware threats of existing SNSs.

2.1 Privacy Threats
Typically, user has to provide SNS with some basic information such as name and email address to create a profile. The majority of SNSs allow registered user to invite their friends whether or not they are member of the SNS. Some SNSs also suggest user to provide them with email account name and password to send invitation to all emails saved on their address books. Once profile is created, user can articulate and share information which is the most specific characteristic of SNS [6]. SNS may offer diverse ways of communications and user can post information in various forms like text, image etc. on their profile [7]. In addition to personal profiles and public pages like those made for celebrity purposes, many companies make use of SNS to keep in touch with their target market. The huge number of users of SNSs and the immense amount of data shared on them have converted social networks to treasures of personal and corporate data. Over and above SNS which has full access to all data, a lot of data can be garnered by both third parties that transmit data and also cybercriminals [8-10].

G’alvez-Cruz [11] defines privacy as a due which allows user to have (1) control of disclosure, (2) control of personal data, and (3) the right of being left alone. Additionally, Cutillo et al. [10] state that an ideal SNS ought to fulfill the following privacy requirements:

- End-to-end confidentiality: All interactions are needed to be confidential and only sender and receiver should have access to data;
- Privacy: Personal information of a user should not be disclosed to any party apart from those explicitly mentioned by the user;
- Access control: User should be able to manage access controls of their profiles as well as attributes of their profiles. User should be also allowed to grant permission to another user or a group of users;
- Authentication: For satisfying the previous necessities, a receiver of a message should be able to authenticate the sender of the message as well as the attribute message;
- Data integrity: For each exchanged message whether it is a response or a request, origin authentication and also modification detection are needed to be performed;
- Availability: Public data has to be always available and all messages should be delivered at any time.

According to Bonneau et al. [12], SNSs with enhanced privacy strategy have better functionality and higher growth rate compared to those with inferior
privacy policy. They also observed that venerable SNSs, vis-à-vis newer ones, have more extensive privacy policy [12]. The threats of SNS, regarding privacy issues can be classified as follows [8, 9]:

1. Browsing user activities: Public personal information on user's profile can be deleteriously downloaded by third parties such as search engines and social network aggregators and consequently pose a risk of developing a history record of user over time [8]. Moreover, even after deleting a profile, owing to established links to other users, some information such as sent messages may still remain available to users who used to be connected to removed user [8, 9, 13]. Furthermore, information about user's online behaviors, like visited profiles, and also the specification of network settings such as the IP address may be monitored and logged by Internet service providers (ISP) and other similar third parties [8-10]. These vulnerabilities could, by unauthorized access to the recorded data, result in privacy leakage risk.

2. Disclosing user's identity: The majority of SNSs encourage users to share a profile image [6]. Shared uploaded images are vulnerable to be examined by face recognition tools that ascertain the real identity of users who create their profiles under pseudonyms [8]. There is also a risk that technologies like Content-Based Image Retrieval (CBIR), by inspecting the specifications of an image, could reveal details such as the place which the image was taken [8, 9]. Moreover, many people may not be aware of usage of their personal images or videos by other users within SNS as in most SNSs user is able to share any images and videos regardless of who in the images or videos are.

User may give a description of each shared file. Furthermore, some SNSs allow user to tag images of other users and link them to the profiles of the owners of the images which enables visitors to get more details by a few clicks [8]. There is, therefore, a high risk of exposing the identity and location of user even sometimes without their knowledge [7]. It is worth noting that some SNSs ask user to provide and share their real name on their profile [14]. Even some suspend users whom their profile has been pseudonymously registered [15]. It is argued by Wisniewski [16] that enforcing user to reveal their real identity on SNS is destructive to privacy of that user.

3. Cyber-stalking, cyber-bullying, harassing, and slandering: The most ideal privacy level is sharing information to only user's friends or a group of users, although, it is still susceptible to cybercriminals who disguise themselves as a friend by using a fake name and image to get access to all information shared by naive users [8].

Particularly, many participants desire to have more friends in their friend list [8] which makes them further vulnerable to cyber-stalking, cyber-bullying, and harassing threats. Stalkers, especially those whose account name has been added to a target user's friend list, may achieve precious information (e.g. date of birth, spouse name, address etc.) from the profile of their victim. Cybercriminals may also keep their targets' activities under surveillance by constantly browsing profiles [8]. Due to several channels of communication of SNS, culprits have...
many options for sending offensive messages, images, videos etc. to intrude on victims' private life. As long as SNS is vulnerable to creating fraudulent profiles, perpetrator is simply able to create false profiles and start posting slanders and canards [8].

4. Eavesdropping: Hundreds of millions of users everyday connect to SNSs from mobile devices [1, 17]. It is also expected that many users connect to the Internet from public places through vulnerable wireless access points. Additionally, most of the current SNSs do not provide secure layer [18] and as a result they pose a risk of transmitted data being captured by sniffing tools.

5. Penetrating into corporate systems: Hackers reconnoiter any resources that help them to penetrate into their victims' systems and SNS is no exception but a valuable asset for tracing and manipulating employees of target corporation for gaining information [8, 9]. A 2010 survey conducted by Sophos found that 59% of employers believe their personnel's behavior on SNS could put their company's security in danger [19].

There are also two architecture styles for managing SNS that impact upon privacy issues. The _rst style is centralized architecture (aka client-server) which is being used by many of SNSs [7]. The second style is decentralized architecture (aka peer-to-peer) that implementing it is not as simple as the centralized style [7].

Centralized style, compared to decentralized architecture, has two big disadvantages as follows: (1) storing the data of a vast number of users in a centralized manner and under only one administrative domain threatens user privacy as a result of inadvertently disclosures, and (2) given that SNS, as a business, seeks to generate proft from its provided services, it has to advertise the products or services of other companies which may thereby make some personal data accessible to third parties [20]. There have been several cases in which advertising companies were provided by SNS with personal information like username of participants who had clicked on advertisements [21]. Conversely, in decentralized architecture, users who store their data in different domains can get connected to each other [22]. Users are, thus, able to choose any servers that provide better services including appropriate level of privacy protection [22]. Above all, in this style users are allowed to keep their information even in their own personal servers [22]. Diaspora [23] is an exemplar of decentralized SNSs.

According to Zhang et al. [7] access control methods of many SNSs are deliberatly weak. They also argue that there is a challenge of making a trade-off between privacy preservation and the following factors:

- Social network searching: It is unattainable to hide all the information of the profile of a user while other users are permitted to find the user through social searching [7]. The same is true of traversing friends' profile [7].
- Social network interaction: The details of a user (e.g. their employment, activities etc.) might be exposed through the profile of their friends [7].
- Data mining: SNS data may be studied for analyzing social behaviors in
which social network is considered as graphs and users are their vertexes and relationships are their edges [7, 24]. To avoid privacy breach and make data anonymous the usual solution is replacing identities of users with meaningless characters [7]. However exploring information of graph topology may pose a risk of the exposure of the real identity of the users [7, 24]. Removing private data on the other hand, reduces the precision of the results [7].

2.2 Malware Threats
The large number of users who are widely distributed across the world and joined with one another by trust relationships and also application sharing feature which some SNSs provide all have made SNSs as an appropriate platform for illegal activities such as spreading malwares [25]. SNS malwares are categorized and discussed below:

1. Spam: Spammer needs to make fraudulent accounts or compromise the account of existing users to propagate spam messages [26]. Spam messages might be sent to user in various ways depending on communication channels of SNS. Spammer may also employ SNS spamming tools and behind some fake accounts with attractive names invite user and send hoax and scam messages to victims in an automated fashion [8]. They typically embed a malicious link in spam message to forward user to a compromised webpage and infect victim' machine by whether exploiting a bug of the installed applications on machines or running a Trojan horse [8, 19]. Cybercriminal may also launch clickjacking attack in the compromised webpage. In clickjacking a malicious frame is put either transparently on or behind a visible webpage containing typical, but fake, objects like buttons and hyperlinks and when user clicks on an object located on the visible page unconsciously executes an unwanted script that is hyperlinked on the transparent frame [27]. It should be noted that user might be reached to the target webpage in multiple stages, after passing multiple intermediate URLs through generic redirectors [28]. Perpetrator might also comment on users' posts on public pages in order to beguile visitors into clicking on malicious link inserted in their comments [8]. Moreover, spammer sometimes uses URL obfuscation technique for hiding real address of the link [26].

In [29] user is allowed to add another user to their friend lists without needing to be consented by the invited user and spammer may, thereby, take advantage of that and share spam messages with the invited user, although, the spammer is not permitted to have access to the private massages posted on the target user's wall. Even in those SNSs that require a two-way friendship relation to be established, once the connection is made, there is a high risk that the spammer will have spam message rapidly spread given that the victim's friends see the message on their friends' profile rather than on a strange webpage [31]. However commonly used methods for confronting email spam such as black-listing IP and domain are not sufficient in SNS since determining whether
an IP or a domain is compromised is a time-consuming process and there is also a possibility of inaccuracy [28, 30]. Moreover, SNS-based solutions like account heuristics are only appropriate for detecting pro_les created by spam and compromised accounts may, therefore, be overlooked by them [28]. Additionally, they need a period of time until a history of the spammed account to be made. [28].

To ameliorate this issue, Thomas et al. [28] have proposed a real-time system, named Monarch, which inspects a URL before it gets published on SNS and grades the URL based on several factors including the specifi_cations of the target webpage.

2. Malicious application: SNSs that allow developers to share their applications are potentially vulnerable to malicious applications that by using social en_ gineering techniques entice users to run them. These malwares are classifi_ed as follows:

- Data stealing application: In some SNSs once a user installs an application, the application has access to the considerable amount of their account's information which poses a risk that the details of user who installs the application are collected by malware's author [25].
- Malicious applet: If SNS provides developer with the feature of sharing Java applets, it may make its users vulnerable to malicious applets that by using some techniques gain access to the disk of a user who has run them [25].
- Survey scam: To install a survey scam application, user typically has to grant it the permission of posting messages on pro_le's wall [32]. This authorization enables malware to advertise itself using victim's pro_le [32]. Once application is installed, by running application and few clicks, victim will be forwarded to a compromised website that tempt visitor into entering bank account details [19, 32].
- Distributed denial-of-service (DDoS) attack: In this technique attacker develops an application which involves Uniform Resource Identi_ers (URI) pointing to resources such as images and videos hosted by victim's server [25]. Once SNS user installs and runs the application, it starts down-loading resources from victim's server and consequently on a large scale there is a high risk of target server being crashed [25].

3. Cross Site Scripting (XSS) attack: In this method, worm's author inserts malicious codes to their pro fi_le and once a user visits the compromised pro fi_le, without the user interaction, the XSS worm makes the pro fi_le of the visitor infected and likewise it spreads the worm [33]. distributed by exploiting the misconfiguration of application programming interfaces (API) whereby users run on their mobile phones to get connected to SNS [34].

4. Command-and-Control (C&C) worm: In this technique, after creating some fake pro_les manually or automatically by zombies [25], hacker uploads their
commands which are normally encrypted to the fraudulent profiles [35, 36].
When a malware developed by hacker infects a machine it makes a connection to each profile specified in the malware code to get the latest commands [35, 36]. A remarkable point to note is that hacker relies on free legitimate servers and consequently blocking the malware connections and also forensic investigation are more difficult than when they use their own domain name and servers for launching attacks.

5. Phishing attack: Phisher can achieve more accurate details about a user through SNS and apply collected information for personalizing and launching attack against the user [8]. Beyond the numerous communication channels of SNSs, knowing the user's personal information such as their address increases the risk of a successful phishing attack as phisher could have greater chance to persuade the user into revealing their confidential information.

3 Proposed Mitigation Approach
The proposed approach is composed of four parts as follows: (1) user education and awareness, (2) privacy preservation strategies, (3) surveillance and ascertainment, and (4) application evaluation and code review which are explained in the rest of this section.

3.1 User Education and Awareness
As we have seen most of the threats of SNS rely on social engineering techniques. Thus educating users, avoiding using convoluted privacy settings, and simplifying warning messages are
It is also advised that legislation on unlawful activities that can be potentially committed within SNS such as computer crimes, copyright infringement etc. to be delineated in privacy policy and terms of use statements. In each country voluntary organizations or institutions can collaborate on collecting and organizing domestic Acts and legislation and provide them for all SNSs to be published on their websites which might thwart some, if not all, perpetrators and most importantly, make users familiar with their legal rights in cyberspace and in SNS in particular. Sending out security newsletters on a regular basis, alarming users regarding malwares that are in progress and above all common social engineering techniques along with methods for counteracting may impede the spread of spam messages, malicious applications, and phishing attacks. Additionally, educating personnel to know how to safely use SNS without posing any threat to the business they work for, rather than obligating them not to use SNS can reduce the risk of corporate data leakage. SNS can prepare a set of proven guidelines to be employed by companies for educating their personnel in regard to SNS surfing.

3.2 Privacy Preservation Strategies
When it comes to privacy preservation, the decentralized architecture outdoes the centralized style. However in both architectures, SNS should, as far as possible, try to meet the privacy requirements cited in Section 2.1. It is also recommended that all data on a user who deletes their account are permanently removed. This includes information that was posted or uploaded by the deleted participant earlier and currently is stored on other profiles or pages that the user used to be in touch with them. Moreover, there are some de-identification techniques [8, 37] that SNS might employ against face recognition tools. SNS may warn users about the risks of sharing personal image on their profiles. SNS, excluding professional-related ones, should also allow user to volitionally choose their profile's name and other details. Furthermore, users who want to have their profile kept secluded should be able to ensconce all their personal data stored on SNS including profile's name and image from social searching, aggregators, and friends of friends. It is also recommended that tagging another user requires the permission of the user.
who is tagged. The user should also be able to remove the tag anytime.
Apart from trade secrets such as spam detecting algorithms, any mechanisms that may potentially expose user's data to any third party should be unambiguously mentioned in privacy policies of SNS.
In case of involvement of a third party like an advertiser or an outsourced monitoring application, SNS ought to employ strategies that prevent the outsider from gaining any data belonging to user through SNS or cookies stored by SNS' website on user's machines. Furthermore, algorithms that insure preservation of edge anonymity should be used in social network graphs in order to keep users' identities confidential.

Regarding eavesdropping threat, all communications between SNS and user need to be encrypted and secured by protocols like the Transport Layer Security (TLS) in order to prevent them to be sni_ed by eavesdropper. Although using these protocols might slow down the transmission process, but applying secure protocols should not be restricted to the login phase as many users may connect to SNS and upload and download their personal information from public places using wireless access points. Many activities of users on SNS will be protected from intermediate third parties and sniffers if transmitted data is encrypted by secure protocols. SNS should implement and follow proper procedures and install efficient security equipments and run appropriate and updated programs for securing and protecting its networks and data stored on its storage systems.

3.3 Surveillance and Ascertainment
It is advised that public pages are separated into two groups, for example, official and unofficial.
For creating an official page, user has to provide SNS with more details to prove the page would belong to the same individual or organization that claims to be. Pages marked as official need to be listed in SNS search result higher than unofficial ones and visitors should be informed that there is no assurance for authenticity of unofficial pages. The same pattern can be applied to normal users. Since 2009 Twitter has implemented a similar method for background check of its prominent users [38].

Categorizing profiles can reduce the number of the visitors of the fraudulent profiles and as spammers and virus authors employ fake profiles to distribute spam messages and application malwares, this method may hinder the propagation progress. SNS might organize volunteers in different areas such as art, politics etc. and they inspect the authenticity of public pages that their owners have requested for official mark. The common method for dealing with cyber-bullying and harassment messages is removing sender by offended user.

Users should nevertheless be able to report libelous and slanderous incidents and SNS needs to take serious actions against offenders like blocking their profile account. SNS may specify that they might provide information to law enforcement agencies and authorized forensic experts for investigation purposes if an offended user files a formal complaint and search warrant is issued.

Conversely, SNS should not violate the freedom of speech and the privacy of any users aside from the defendant. Furthermore, beyond the existence of a mechanism for blocking fake accounts, users should be able to report comment-spam messages as well. With regard to blocking spam messages, compared to blacklisting domain and account heuristics methods, Monarch is more propitious as in addition to examining the URL, it checks the attributes and specifications of the target webpage. It is also suggested that when the number of times that the same message has been sent to users reaches a predetermined value, SNS provides new users who receive the message with a statistics options that demonstrate the number of users who have reported the message as spam. It is obvious that this value should be far less than the value that SNS considers for blocking spam messages.

Finding profiles compromised with C&C commands is not an easy task as hackers may use common words that any other users might enter in their profile. However attackers often make numerous profiles and right after that thousands connections are made to their profiles. It is not unusual thousands users visit a profile but when lots of connections are made to a profile which its age is only few hours, SNS can employ methods like Completely Automated Public Turing Test To Tell Computers and Humans Apart (CAPTCHA) [39] to verify whether the profile is requested by a human or a computer program. Virus' author may, however, handle the situation by either increasing connection time interval of zombies or limiting the number of zombies that connect to a profile. Consequently, SNS should repeatedly explore C&C malwares and, if possible, establish a joint venture with anti-virus software developer companies for having precise details of the structure of new variants of this kind of...
malwares and update the connection limitation control.

3.4 Application Evaluation and Code Review

With reference to malicious applications, the most sophisticated solution is that SNS experts investigate application including its source codes before it is shared. Application should have access to user' details as little as possible. SNS may fully inform users about data that are collected by the requested application. Moreover, there should be a feature that allows users to report suspicious behaviors of applications. Users also need to be able to delete any applications anytime. There should be also proper procedures that enable third parties that their servers are under attack of SNS application to report incidents.

XSS worms have been one of the most challenging malwares on the Internet. Unless the codes of all webpages and web applications are examined and tested thoroughly, SNS are very vulnerable to XSS worms and other types of cyber attacks like SQL injection. Thus rather than enabling users to add scripts like JavaScript codes, SNS can provide them with graphical user interfaces (GUI) that allow user to design their profile without having access to page codes.

Code testing and preventing users having direct access to their profiles' codes are the finest way for dealing with XSS worms. Application testing can also reduce the number of SNS malwares like data stealing applications, malicious applets, survey scams, and those used for DDoS attacks.

Table 1 summarizes the threats that are addressed by the recommendations of this work. Although the proposed mitigation approach relies on having many regulators who constantly support users, audit public pages, and test applications, but it is believed significant parts of these jobs can be done by voluntary users.

4 Conclusion and Future Work

To date, privacy preservation strategies applied to the existing SNSs have not been effective enough to secure personal data from being intruded. Moreover, SNSs are highly vulnerable to be abused for malware and spam propagation purposes except if they employ proper controlling and monitoring mechanisms. It has been discussed that user awareness is a key factor which can considerably

Table 1. The proposed approach in relation to the studied threats

<table>
<thead>
<tr>
<th>Threat</th>
<th>Education and Awareness</th>
<th>Privacy Strategies</th>
<th>Surveillance</th>
<th>Application Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsing user activity</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Disclosing</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
diminish many identified risks.
The presented approach suggests practical methods for preserving user data and deterring virus authors to spread malwares through SNS. It also complies with the definition of privacy cited in Section 2. More research should be undertaken on preventing shared personal information from being reuploaded by users who are not the owner of the information. Furthermore, the criteria of courts to have jurisdiction over SNS-related cases whereby SNSs should be subject to their judgments are open to dispute. We will continue to improve the work and hopefully it will eventually, by further research, lead to development of a comprehensive framework for securing SNS.

References


