Ramiz H. Shikhaliyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az

DOI: 10.25045/jpis.v07.i2.08

SECURITY ISSUES IN SOCIAL NETWORKS

Nowadays, a large number of social networks exist in the Internet. These social networks are very popular and play a prominent role in people's life. Alongside, the social networks have also caused the occurrence of new threats in the field of information security. Such threats are related to the distribution of malicious software and spams, attacks on social engineering and social network accounts, tracking, fraud and etc. This article is dedicated to the analysis of existing threats in social networks and the protection issues against them.

Keywords**:** *social network, malicious software, spam, phishing, fake account.*

Introduction

Internet has become a main tool of global communication and information exchange among people. The establishment and rapid development of *Web 2.0* technology has substantially broadened the capabilities of Internet and facilitated the access of people to social networks regardless their geographic location [1]. In turn, the rapid development and broad use of social networks has turned it into one of the main elements of *Web 2.0* technology.

Social network is a service which facilitates the establishment of connections and information exchange among people. At present, several social networks, such as *Facebook, Twitter, Linkedin* and etc. exist. These social networks become popular day by day, and play an important role in the society's life. Depending on user interests, various specialized social groups – for example, business-oriented networks, such as *LinkedIn* and *Xing*, are created, which enable the users to establish business relations and to propose job opportunities. Some social networks are only oriented to the establishment of communication among people and act as an environment for virtual encounters. However, social networks bring out new problems related to the immunity of private lives of users and the information security. That is, the creation of social networks has led to the increase of security risks. These risks are related to the problems of different aspects such as the expansion of malicious software and spams, the attacks on social engineering and social network accounts, as well as tracking, fraud, blackmailing, smearing and etc. Alongside with indicated threats, social networks can also incur various threats to national security depending on the interests of users [2].

On the other hand, the number of social network users have rapidly increased and exceeded 2 billion people in recent times. According to forecasts, the number of social network users will reach 2,5 billion people in 2018 [3]. Such popular use of social networks and generation of a large volume of information by users has turned them into a target for attacks by malignant persons and offenders. Social networks are used by malignant persons as a favorable platform for conducting various kinds of attacks from spamming [4] till individual phishing [5] attacks. Naturally, the maintenance of information security and secure use of social networks in Internet environment have become a topical issue in such situation. Hence, the analysis of information security, social-aspect threats and the protection methods from those in social networks are of great importance. Such analysis assumes large importance in terms of the maintenance of information security and the secure use of social networks by people in the Internet environment.

Social network threats

The security in social networks mainly covers the issues of protection of users' personal information from malignant acts. For this purpose, social network users must be aware of the risks and threats related to their personal information.

The threats that can occur in social networks may be divided into four groups. The first group includes the conventional threats, especially the threats related to the immunity and security of private life. These threats cause danger not only for social network users, but also for other Internet users who do not use social networks. The second group captures the modern threats related to the immunity and security of private lives. These threats mainly pertain to social networks, and cause a danger for immunity and safety of private lives by using the social network infrastructure. The third group covers the combination of various threats, that is, more sophisticated and dangerous attacks can be conducted as a result of combination of various threats. The fourth group contains the threats with social aspects. Tracking, fraud, blackmailing, smearing and etc. can be attributed to such threats.

Conventional threats remain as a problem since the beginning of the broad use of the Internet. Malicious software [6], spams [7], phishing [8] and etc. can be attributed to such threats. Those can be very dangerous depending on the structure and the character of social networks and may be spread to several user computers in short time. Such threats can cause a danger to users, as well as their "friends" by using the personal information of user posted in social networks. For instance, by using the details of users in Facebook profiles, malefactors may generate spam-information, which can be attractive at first sight and locate a malicious software code into such information. Considering that, such information is of personal character, it can be surely said that some user will open it and his/her computer will be infected with malicious software. In the majority of cases, the target of such threats is the daily and important user resources. These resources include credit card credentials, account passwords, computing power, impact zone and etc. Additionally, those threats may use the obtained information for forwarding information on behalf of the user of infected computer and even change the user's personal data.

The aim of creating malicious software is to collect the registration data of users and disrupt the performance of computer in order to gain access to individual information. In order to distribute such programs among users and their "friends" in social network, the structural features of social networks are applied. In some cases, malicious software programs use the registration data of users in order to send infected information to their "friends".

First malicious software spread in social networks such as *Facebook*, *MySpace* and *Twitter* was *Koobface* worm. While infecting, *Koobface* worm attempts to capture the registration data of users and to connect infected computers to botnet network [9]. Computers connected to botnet become "zombies" and thereafter, are used for malignant purposes such as spamming, attacks on other computers and services connected to Internet and etc.

Phishing attacks are attributed to social engineering attacks, and used in order to obtain confidential information and personal credentials of users. For this purpose, an attacker acts as a reliable third party. Usually, social network users are exposed to phishing attacks due to their own sociality and naivety [10]. Hence, the attempts of phishing attacks have increased in social networks in recent periods. According to the Microsoft report on security [11], the target of 84,5% of phishing attacks, occurred in the Internet, were social network users.

Spams are unwanted information of advertising type sent by the user called "spammer" to other users by using electronic information exchange systems. Social network spammers use the platform of social networks for spreading spams. For this purpose, spammers create fake profiles in a social network [12]. Additionally, spammers may use the social network platform in order to add the information of comment type in pages, while a large number of users review these pages.

The modern social network threat pertains solely to this environment. Usually, the target of such threats is the personal data of social network users, as well as their "friends". For example, malignant persons create a fake "friend" profile in order to attack the personal information of the *Facebook* user and send requests. If the target users accept the request of this "friend", his/her personal data is exposed to a threat and malefactors are able to capture them. Additionally,

malicious persons are able to extract some information regarding the "friends" of the *Facebook* user by compiling and analyzing the information pertaining to those.

Existing modern social network threats are carried out according to various scenarios. For example, an attack called *ClickJacking* deceives users by inducing to click at first sight useful, but malicious links. By using *ClickJacking,* malignant persons may spread spams via "likes" by manipulating the users (this is also called *likejacking*) [13]. As an example to *ClickJacking* attack, "Don't click" attack may be shown which occurred in *Twitter* in 2009. Violators have located masked (actual URL was hidden) URL address (a locator showing the address and location of a file or resource in Web) with "don't click" information in *Twitter*, and as Twitter users entered this link, the information was spread as a virus and located in user accounts [14].

The majority of users in social networks use pseudonyms in order to maintain the privacy and anonymity. Malignant persons use the attacks called "de-anonymization" against them. During this attack, wrongdoers use malicious cookies (it is the technology storing and entering the information in user devices such as computers, tablets or mobile phones), the methods of tracking of network topology and user groups. Alongside, it is possible to identify them by the analysis of the information leak from social network websites [15]. Another method of "de-anonymization" is solely constituted of the analysis of the social network user membership in groups [16]. This method is tested in Xing social network, and as a result, 42% of users were identified. Another method is based on the comparison of user profiles of various social networks [17].

Usually, social network users post the photos of themselves and their "friends". For example, millions of photos are posted daily in *Facebook* social network [18]. Additionally, the viewing and opening of photos of the majority of Facebook users' profiles is public. For example, *Faces of Facebook* website [19] allows to view the profile pictures of more than 1,2 billions of Internet users. These photos can be used for the creation of biometric database and the identification of those social network users without their consent.

Fake profiles (also called as "social bots") imitate the human behavior in social networks as automatic or semi-automatic profiles. Mostly, such fake profiles are used for collecting personal data of social network users. For this purpose, social bots generate "friend" requests for social network users, and they accept these requests in most cases. As a result, social bots obtain an opportunity to gain access to personal data of users while the personal data of social network users is usually accessible for his "friends" only. Alongside, fake profiles can be used for conducting *Sybil* attacks [20], the spread of social spams [21] and etc. An attacker uses the reputation points of a person in order to manipulate by creating several identificators (*Sybil*).

Nowadays, malignant persons may conduct more sophisticated and dangerous attacks by combining traditional and modern threats. For example, they can purposefully collect the passwords of Facebook users by phishing and post the information possessing *ClickJacking* attack. Hence, the malefactors become capable to induce "friends" of users to disclose the information by deceiving them and locate viruses in their computers.

Several threats of social character exist in social networks and tracking, fraud, blackmailing, smearing and etc. pertain to those. Unfortunately, some people use the social networks in order to conduct such threats against other people. For this purpose, malignant persons benefit from personal data of social network users and various attack tools. In some cases, such threats are even used against different countries, organizations and etc., and the number of social threats has increased.

Tracking in social networks is one of the most widespread and well-known threats of social character. While conducting such threats, malignant persons may obtain the personal data (location, phone number, work schedule, home address and etc.) and their profiles. They may impact the targeted users in different ways. For example, this impact may start with frightening people and evolve to blackmailing, privacy violation and even serious physical damage (for example, terror), psychological shocks and etc.

Protection methods against threats in social networks

Recently, various solutions have been proposed for the protection against threats in social networks. Such solutions capture different levels, that is, social network operators, security companies and the proposals of scientific researchers.

Social network operators carry out various security measures for maintaining users' safety. For instance, authentication mechanisms and several measures such as the regulation of personal data are applied.

The mechanisms of authentication are applied to ensure that social network users are neither the social bots nor notorious user accounts, but real persons. That is, the authentication enables to ensure that real persons have registered in and entered social networks. For this purpose, various authentication mechanisms such as *CAPTCHA* (*Completely Automated Public Turing Test to Tell Computers and Humans Apart*) [22], the identification of an image of "friends", that is the recognition of a "friend" among the images presented to suspicious user; multifactor authentication [24], that is, the entrance of additional information by users alongside with password and etc. are applied. Such authentication mechanisms enable to prevent the capture of personal data of users by malignant persons via social bots and notorious user accounts and the spread of malicious software and spams.

The majority of social networks facilitate the users to control their personal data. This enables the users to protect their personal data from other users [25, 26]. For example, Facebook users can control their personal information and manage the permission to view those, i.e he or she can specify the user groups ("friends", 'friends of friends" and "everyone") who can view other personal information [27]. Some social network operators also enable the users to carry out additional security configurations. These configurations allow the users to activate the secure view by users of their own personal data, to receive notifications about the access to their account and set other security features [28]. Notwithstanding this, most users are not able to manage the parameters of privacy settings of personal data and expose their personal data to threats [29].

Some social network operators apply additional internal security mechanisms in order to maintain the user privacy. Such safety mechanisms allow to be safe from the spread of spams, fake profiles, fraudulency and etc. threats [30]. For example, in order to prevent malicious attacks and unauthorized data collection, *FIS* (*Facebook Immune System*) is applied [31]. FIS carries out the analysis and classification of reading and writing operations in *Facebook* database, in real time regime.

Social network operators have added an option of information sharing in social websites in order to protect the users of certain groups, mainly children and teenagers from being followed by other users [34]. In some countries, for example, they have added "Panic Button" to Facebook in order to protect children in social networks. Alongside, some social websites cooperate with certain organizations in order to protect potential victims (for example, children). For instance, Facebook has added a button for reporting regarding the suspicious behavior or abuse based on the request of the Organization of Children Protection of Great Britain in 2010.

Several commercial solutions have been proposed by well-known companies in security sector for the protection against threats in social networks. For example, *AVG, Avira, Kaspersky, Norton, Panda, McAfee, Symantec* and etc. security companies have presented various Internet-security software to social network users. Usually, such solutions include antiviruses, internetwork screens and other Internet-security programs. Corresponding measure allows the social network users to protect their computers against the attacks such as malicious software, botnets, *ClickJacking*, phishing and etc. type. For example, *AVG PrivacyFix* software tool as a mobile application and web-browser add-in [34] allows *Facebook, LinkedIn* and *Google* users to control their personal data. *Norton Safe Web* [35] software as *Facebook* application searches for new

"friends" of users and informs them regarding the malicious links and websites. *McAfee Social Protection* [36] software as a mobile application enables the users to protect the images posted in *Facebook* pages by users, to view and download those images by other users.

Various solutions presented by scientific researchers in order to provide protection against the social threats in social networks are based on the investigation of social network threats. These measures are mainly oriented to the detection of malignant users and malicious application. Suggested solutions can be used for the maintenance of privacy of users by social network operators.

In recent years, several research works have been carried out regarding the safety of social networks, that is, the protection of personal data, phishing, spams, detection of cloned or fake profiles and etc. areas. For example, *Audience View* interface was proposed for *Facebook* [37]. This interface allows the users to view their profiles as other users, for example, as "friends" or others. Such interface enables to detect which data is accessible for other users and to control the interface of personal data. The maintenance of user privacy in social networks is one of the important issues and *FaceCloak* architecture was proposed in this regard [38]. According to the architecture, the personal data of user is protected from social network users, as well as other users. For this purpose, *FaceCloak* stores the private information in a separate server in an encrypted format. Another important issue is the maintenance of the privacy of users for which a template for the creation of a tool for the maintenance of social privacy is proposed [39]. This template allows the automatic control of personal data of social network users.

The majority of methods proposed regarding the fight against phishing attacks are based on the methods of detection of phishing websites and phishing links [40-42]. As the number of phishing attacks grows in social networks, several methods are developed for the identification of those. For instance, a system for detecting suspicious URL's called *WarningBird* was developed for *Twitter* [43]. This system allows to detect phishing attacks "hidden" behind the redirecting URLs.

A large number of solutions have been also proposed for spam detection in social networks. For example, an algorithm was developed for the detection of video-spams [44]. This algorithm allows for detecting spams in *YouTube*. Moreover, for the classification of spams in *Twitter* social network, the employment of the features of content and social network scheme was proposed [45]. Also, the algorithm of machine learning was employed for the detection of spams in social networks.[46]. The algorithm of machine learning allows to detect various types of spams.

Different methods and approaches were proposed for the detection of cloned profiles in social networks. For instance, a specific tool was developed in order to determine whether the profiles of social network users have been subject to cloning attack [47]. An approach called *CloneSpotter* was proposed in order to detect the cloning attack on social network profiles [48]. This approach is based on the analysis of registration data of users available for social network operators.

Various approaches have been proposed regarding the detection of fake profiles in social networks. Those approaches include various algorithms, methods and tools for the detection of fake profiles and the prevention of different *Sybil* attacks [49]. Although the goal of the algorithm of spotting the fake profiles and the algorithm protection from the Sybil attacks - the detection of fake profiles, is similar, some differences are present. The algorithm of spotting the fake profiles is oriented to the detection of fake profiles, and the cybercriminals possessing several fake profiles in social network. The algorithm of protection against *Sybil* attacks is aimed to identify the malignant persons creating several fake profiles in social networks. For this purpose, *SybilGuard* [50] and *SybilLimit* [51] protocols were developed. Alongside, an algorithm called *SybilInfer* was developed that allows to spot "real" and "fake" users in social networks [52]. Another approach is the employment of structural features of social networks for the verification of users; for this purpose, *SybilRank* tool was presented [53].

Conclusion

Nowadays, social networks have become an integral part of everyday life of people. The majority of Internet users spend the large share of online activity in social networks. People establish contacts and share information (information, images and video) and experiences via social networks. Alongside, various threats exist in social networks. Hackers, swindlers and etc. use social networks as a tool for finding new "victims" and conducting their malignant acts. Hence, the analysis of existing threats in social networks and the ways of protection from those are of high topicality.

The article analyzes the threats existing in social networks and the methods of protection. As a result of the analysis, it can be concluded that the threats existing in social networks pertain to two categories: traditional information security problems and threats with social aspects. It is also worth mentioning that, regardless the attribution of the problem to any group, those are directed towards the violation of private lives of users. It can be said that the violation of privacies of people in social networks, i.e in virtual reality, directly affects their real life.

The outcomes of the analysis on the threats existing in social networks and the protection methods may facilitate the secure use of social networks by people and the selection of tools and solutions for the maintenance of the safety of users by social network operators.

References

1. Stern J., Introduction to web 2.0 technologies, http://www.wlac.edu
2. Imamverdiyev Y. Social media and security issues / II Republican scientific-practical conference on multidisciplinary problems of Information security dedicated to 150 years' anniversary of International Telecommunications Union, 2015, pp. 189-192.
3. http://www.statista.com/topics/1164/social-networks/
4. Stringhini G., Kruegel C., Vigna G., Detecting spammers on social networks / Proc. of the 26th annual computer security applications conference, 2010, pp. 1-9.
5. Jacoby D., Facebook security phishing attack in the wild, https://securelist.com/blog/events/31951/facebook-security-phishing-attack-in-the-wild-14
6. https://en.wikipedia.org/wiki/Malware
7. https://en.wikipedia.org/wiki/Spamming/
8. https://en.wikipedia.org/wiki/Phishing
9. Baltazar J., Costoya J., Flores R., The real face of koobface: The largest web 2.0 botnet explained, Trend Micro Res., 2009, vol. 5, no. 9, 10 p.
10. Amin T., Okhiria O., Lu J., An J., Facebook: A comprehensive analysis of phishing on a social system, EECE 412 Term Project Report, 2010, 6 p., http://www.courses.ece.ubc.ca/412/term_project/reports/ 2010/facebook.pdf
11. Cavit D. Microsoft security intelligence report, 2010, vol. 10, 89 p. http://www.microsoft.com/en-us/download/details.aspx?id=17030
12. Fire M., Katz G., and Elovici Y., Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies / ASE human journal, 2012, vol. 1, no. 1, pp. 26-39.
13. Lundeen R., Ou J., Rhodes T., New ways I'm going to hack your web app // Proc. of the Blackhat AD, 2011, pp. 1-11.
14. McMillan R., Researchers make wormy twitter attack / PCWorld, 2009, http://www.pcworld.idg.com.au/article/296382/researchers_make_wormy_twitter_attack/
15. Krishnamurthy B., Wills C. E., On the leakage of personally identifiable information via online social networks // Proc. of the 2nd ACM workshop on online social networks, 2009, pp. 7-12.

16. Wondracek G., Holz T., Kirda E., and Kruegel C., A practical attack to de-anonymize social network users // Proc. of the security and privacy IEEE symposium, 2010, pp. 223-238.
17. Peled O., Fire M., Rokach L., Elovici Y. Entity matching in online social networks // Proc. of the international conference on social computing, 2013, pp. 339-344.
18. Facebook, Form 10-k (Annual Report)—Filed 02/01/13 for the Period Ending 12/31/12, 2013, 139 p., http://files.shareholder.com/downloads/AMDA-NJ5DZ/2301311196x0 xS1326801-13-3/1326801/1326801-13-3.pdf
19. The Faces of Facebook, http://www.app.thefacesoffacebook.com/
20. Douceur J. R., The sybil attack // Proc. of the 1st international workshop on peer-to-peer systems, 2002, pp. 251-260, http://www.dl.acm.org/citation.cfm?id=646334.687813
21. Gao H. Detecting and characterizing social spam campaigns // Proc. of the 10th ACM SIGCOMM conference on Internet measurement, 2010, pp. 35-47.
22. Boshmaf Y., Muslukhov I., Beznosov K., and Ripeanu M., The socialbot network: When bots socialize for fame and money // Proc. of the 27th annual computer security applications conference, 2011, pp. 93-102.
23. Jeffries A., Facebook's security check asks users to identify photos of friends' dogs, Gummi Bears [UPDATED], 2010, http://readwrite.com/2010/08/04/facebooks_security_check_asks_users_to_identify_ph
24. Song A., Introducing login approvals, 2011, https://www.facebook.com/note.php?note_id=10150172618258920
25. Liu Y., Gummadi K., Krishnamurthy B., and Mislove A., Analyzing Facebook privacy settings: User expectations vs. reality // Proc. of the ACM SIGCOMM conference on Internet measurement conference, 2011, pp. 61-70.
26. Mahmood S., Desmedt Y., Poster: Preliminary analysis of google+'s privacy // Proc. of the 18th ACM conference on Computer and communications security, 2011, pp. 809-812.
27. Facebook, Facebook Help Center: Privacy, http://www.facebook.com/help/privacy
28. Axten S., Staying in control of your facebook logins, https://www.facebook.com/notes/facebook/staying-in-control-of-your-facebook-logins/389991097130
29. Fire M., Kagan D., Elyashar A., and Elovici Y., Friend or foe? Fake profile identification in online social networks / Springer journal of social network analysis and mining, 2014, vol.4 no.1, pp. 194-216.
30. Chowdhury A., State of twitter spam, 2010, https://blog.twitter.com/2010/state-twitter-spam
31. Stein T., Chen E., and Mangla K., Facebook immune system // Proc. of the 4th workshop on social network systems, 2011, pp. 1–8.
32. Facebook, Report abuse or policy violations, https://www.facebook.com/report
33. Axon S., Facebook Will Add a Panic Button for U.K. Teens, Jul. 2010., http://www.mashable.com/2010/07/11/facebook-panic-button-ceop
34. AVG, Avg Privacyfix: http://www.privacyfix.com
35. Symantec, Norton Safe Web: https://www.facebook.com/appcenter/nortonsafeweb
36. McAfee, Mcafee Social Protection Beta: https://www.protectmediaonline.com
37. Lipford H. R., Besmer A., Watson J., Understanding privacy settings in facebook with an audience view // Proc. of the 1st conference on usability, psychology, and security, 2008, pp. 21-28.
38. Luo W., Xie Q, Hengartner U, FaceCloak: An architecture for user privacy on social networking sites, // Proc. of the international conference on computational science and engineering, 2009, vol. 3, pp. 26-33.
39. Fang L., LeFevre K., Privacy wizards for social networking sites // Proc. of the 19th international conference on world wide web, 2010, pp. 351-360.
40. Garera S., Provos N., Chew M., Rubin A. D., A framework for detection and measurement of phishing attacks // Proc. of the ACM workshop on recurring malcode, 2007, pp. 1-8.

41. Ma J., L. Saul K., Savage S., Voelker G. M., Beyond blacklists: Learning to detect malicious web sites from suspicious urls // Proc. of the 15th ACM SIGKDD international conference on knowledge discovery and data mining, 2009, pp. 1245-1254.
42. Xiang G., Hong J., Rose C. P., Cranor L., CANTINA+ A feature-rich machine learning framework for detecting phishing web sites / A ACM transactions on information and system security 2011, vol. 14, no. 2, pp. 1-28.
43. Lee S., Kim J., Warningbird: Detecting suspicious urls in twitter stream // Proc. Of the 19th Annual Network & Distributed System Security Symposium, 2012, pp. 1-13.
44. Benevenuto F., Rodrigues T., Almeida V., Almeida J., Gonzalves M., Detecting spammers and content promoters in online video social networks // Proc. of the 32nd international ACM SIGIR conference on research and development in information retrieval, 2009, pp. 620-627.
45. Wang A., Don't follow me: Spam detection in twitter // Proc. of the international conference on security and cryptography, 2010, pp. 1-10.
46. Aggarwal A., Almeida J., Kumaraguru P., Detection of spam tipping behavior on foursquare // Proc. of the. 22nd international conference on World Wide Web, 2013, pp. 641-648.
47. Kontaxis G., Polakis I., Ioannidis S., Markatos E., Detecting social network profile cloning // Proc. of the IEEE international conference on pervasive computing and communications workshops, 2011, pp. 295-300.
48. Shan Z., Cao H., Lv J., Yan C., and Liu A., Enhancing and identifying cloning attacks in online social networks // Proc. of the 7th international conference on ubiquitous information management and communication, 2013, pp. 17-19.
49. Koll D., Jun Li, Stein, J., Xiaoming Fu, On the state of OSN-based Sybil defenses // Proc. of the IFIP networking conference, 2014, pp. 1-9.
50. Yu H., Kaminsky M., Gibbons P., and Flaxman A., Sybilguard: Defending against sybil attacks via social networks // Proc. of the conference on applications, technologies, architectures, and protocols for computer communications, 2006, vol. 36, no. 4, pp. 267-278.
51. Yu H., Gibbons P. B., Kaminsky M., and Xiao F., Sybillimit: A nearoptimal social network defense against sybil attacks / IEEE/ACM transactions on networking, 2010, vol. 18, no. 3, pp. 885-898.
52. Danezis G. and Mittal P., Sybilinfer: Detecting sybil nodes using social networks // Proc. of the 16th annual network & distributed system security symposium, 2009, 16 p.
53. Cao Q., Sirivianos M., Yang X., Pregueiro T., Aiding the detection of fake accounts in large scale social online services // Proc. of the 9th USENIX conference on networked systems design and implementation, 2012, p. 15.