International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering Vol. 2, No. 1, 2015, pp. 1-10.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

Assessing security challenges in online social networks

Marjan Amiri[a] , Abbas Akkasi[b]

[a]*Islamic Azad University, Electronic Unit, Tehran, Iran.*

Abstract

The cyberspace of online social networking is one of the most important tools to manifest the effects of globalization. This cyberspace creates a wide field for information and different semantic emergence. Users spend most of their time on social networks, and what is discussed in few past years is the security of users and preserving their privacy in these social networks. Increasing the use of social networks and sites, users are faced with various problems that security issues in cyberspace as well as users' privacy preservation in social networks are as the most important ones. In relation to privacy and security in social networks, numerous articles have been written, each of them has assessed the issues. This article examines several papers which have addressed security challenges in these networks, and solutions to enhance the security of networks, and it examines each of these articles, and discusses their positive and negative points, and finally, a conclusion based on these papers is presented.

Keywords: Online Social Networking (OSN), Issues of Privacy, Security Challenges

Introduction:

Various societies affected by the massive scientific-technological developments are moving toward the information or networking society. Networking society is a society which is structured by the technology. Regarding popularity among users and the vast geographical scope within national boundaries, virtual social networks have become personal and private communication without any control of authorities, and they have created effective areas beyond the control of governments and authority organizations in societies [Wiki].

The first internet social networking site was in 1997 that called SixDegrees.com. This site allowed users to create profiles, and they could provide a list of their friends. But it was not a successful project, and it stopped after three years. Then, this process started in 2001, and various social networks were formed, for instance, Ryaz network was formed for the purpose of trade and business, and after that the emergence of different social sites that have been created for different purposes and applications continued (Including organizing various virtual social groups, online targeted advertising, developing social contributions, sharing favorites by members, creating content by members, accelerating cultural communication, and a useful tool to identify mental disorders). By 2008, Facebook social network was launched that has become the world's largest social network at present and many people around the world are members of this network.

In 2005, we saw the emergence of laws to this social network. Because a lot of personal information was placed on these sites, laws should be created to protect and provide security for the data. Because we face with new vulnerabilities in the security area of exchanging information, including lack of users' awareness and increasing the number of social networks. Many users are active in the networks regardless of the risks and security threats that could jeopardize their privacy. Just in 2010, more than 286 million new threats have been identified in cyberspace, that they are unprecedented in terms of the number, complexity and scope [.hamshahri].

This article has reviewed some other articles in the field of security in social networks and it attempts to criticize each of the articles as much as possible, and takes the pros and cons of each paper. This study was conducted on five papers. These articles have been ordered by publishing date and they start from old to new and section 2 is definition of social networking. Section 3 refers to the article and studies and efforts that article has done, in Section 4, discussions or criticism about each of the articles are mentioned, Section 5 is about the conclusions of these studies, and references of this article are stated in section 6.

1. Definition of social networks

Social network is a social structure made of nodes (which are generally individual or organizational) connected to each other by one or more specific types of dependence, such as ideas and financial transactions, friends, relatives, Web links.



Social network analysis considers social relationships in terms of nodes and ties. Nodes are Individual actors within the network and ties are the relations between these actors. A great variety of ties can exist among nodes. According to various studies, the capacity of social networks can be used in many individual and social levels in order to identify problems and determine solutions, hold public relations, govern organizational affaires, make policy and guide individuals toward achieving the goals.

In the simplest form, a social network is the mapping of all the ties among the nodes of the study. Social networks can also be used to detect the status of each user. These concepts are often displayed in a social network diagram in which points are nodes and lines are the marker of ties [Wiki].



2. Assessing articles

2.1 Security and Privacy in Online Social Networks: Challenges and Opportunities

Regardless of the social networking purpose, one of the main incentives for users to join a social network is to create a profile and to use social networking services, such as: sharing information, communicating with others, but disclosing personal information in social networks is double-edged sword. This article assesses the security and privacy in social networks. According to this article, there are two architectures on the social network: Client Server and P2P. This article has divided the privacy in social networking into several categories (user anonymity, preserving user's privacy, user's communications privacy, data integrity and authentication), and the enemies of social networks into two inner invaders, and external invasion or external intruders. According to this article, social networking sites to search more efficiently should disclose more information from users' profiles that is a violation of user's privacy. This paper discusses Client Server architecture against P2P architecture in social networks, and it is said that a client-

server architecture is better than is P2P, for example, when a person searching for his friend, centralized architecture is better, even for data mining, but inserting all information in one place may violate privacy and have some risks while this issue is largely considered in P2P architecture. In this architecture, the encrypted data is stored but the cores of P2P is dispersed, currently, it is difficult to be implemented because it is hard to collect information, and for these reasons, the owners of social networks don't tend to search it [C .zhang et al,2010].

3.2) security issues in online social networks

This paper examines the current state of security and available defense mechanisms for the popularity of social networking, the authors have divided attacks to four categories (privacy breaches, viral marketing, and the attacks of network structure, malicious attacks), and primarily the focus is more on privacy concerns. This paper examines the users of social networks in Carnegie Mellon University.
In this article, the violation of privacy has four branches (Invading privacy by service providers, violating privacy by other users, Invading privacy by applications, identification and anonymity).
This article focuses on viral marketing method (a way of advertising companies and commercial institutions in social networks and the Internet) that causes three types of attacks (spam on social networks, phishing and user account attacks), and defense mechanisms discussed in social networks are divided to three sections (diagnosis, demotion, prevention), and one point, security mechanisms is more on the client side and it has discussed to attack the Sybil (an attack on a network structure), and then it has paid attention to three defense mechanisms (trusted certification, supply testing, periodic costs), next to malicious attacks (Malware). In Table 1, the attacks on social networks are compared with the rate of threats and knowledge and effective defenses against each attack.

1. comparing social network attacks

Measure	Information leak	De-anonymizing	Phishing	Sybil	Malware	Spamming
Attack difficulty	Easy to medium	Medium	Easy	Hard	Hard	Easy
Server defense effectiveness	Yes, but with limited effectiveness	No	No	Yes	Yes, but with limited effectiveness	Yes
User defense effectiveness	Yes	No	Yes	No	Yes, but with limited effectiveness	No
Threat to user	High	Medium to high	High	Medium	High	Low

3.3) privacy and national security issues in social networks: Challenges

This paper investigates the structure and characteristics of profiles' members and the challenges about private matters which individuals and their governments and companies in the social networks are faced with, how they can be used to define national security, how to become a new weapon for mobilizing masses and also how social networks are turning to forces for revolution and social justice. Business tools for cyber criminals are intelligent and indirect (such as creating the fake profiles of friends, hacking friends' profiles and sending emotional message from a friend and the emails known as computer hostile code (Malware)).
Various social networks have been examined in nine cases (Social networks based on the profile, content-based social networking, white label social network, multi-user virtual environments, mobile, micro-blogs / offering updates, social search, and topical websites). Table 2 is the result of a research carried out in this article about what information is in the user's profile.

2. Information that users insert in their profiles

Profile Information	**Facebook**	**Twitter**	**9jabook**	**LinkedIn**	**Orkut**	**Friendster**	**Tribe**	**MySpace**
Photo	*	*	*	*	*	*	*	*
Professional Detail	*	*	*	*	*		*	
Gender	*	*	*	*	*	*	*	*
Age/Date of Birth	*	*	*	*	*	*	*	*
Sexual Orientation					*			*
Marital Status	*	*	*	*	*	*		*
Sense of Humor					*			
Hobbies/Interest	*	*	*	*	*	*	*	*
Favorite Music	*		*	*	*	*	*	*
Favorite TV	*	*			*	*	*	*
Favorite Books	*	*			*	*	*	*
Favorite Food					*			
Location	*	*	*	*	*	*	*	*
Home Town	*	*	*	*	*	*	*	*
Here for…				*	*	*	*	*
Schools	*	*	*	*		*	*	*
College/University	*	*	*	*		*		
Clubs &Organizations	*	*	*				*	
Languages	*	*	*	*			*	
Religion	*	*	*	*	*			*
Smoking					*	*		*
Drinking					*	*		*
Nationality	*	*		*	*	*	*	*

In this article, recommendations have been mentioned to enhance the security of social networking users, and it has addressed privacy issues in nine cases (viruses, tools, identity thief, the social engineering of attacks, third-party applications, using information business, professional reputation, personal relationships, personal safety). Finally, it focuses on the national security issues, being jeopardized with the increasing development of these networks [S.Abdulhamid et al, 2011].

3.4) Security and Privacy in Online Social Networks

This paper aims to consider a specific issue encompassing advanced researches in the field of security and privacy in social networks and sharing technology in accordance with the latest scientific developments in order to achieve progress in the security of social network. This article examines four other papers considering new technologies and methods to confront with constructing security, managing social networks and relevant secure program.

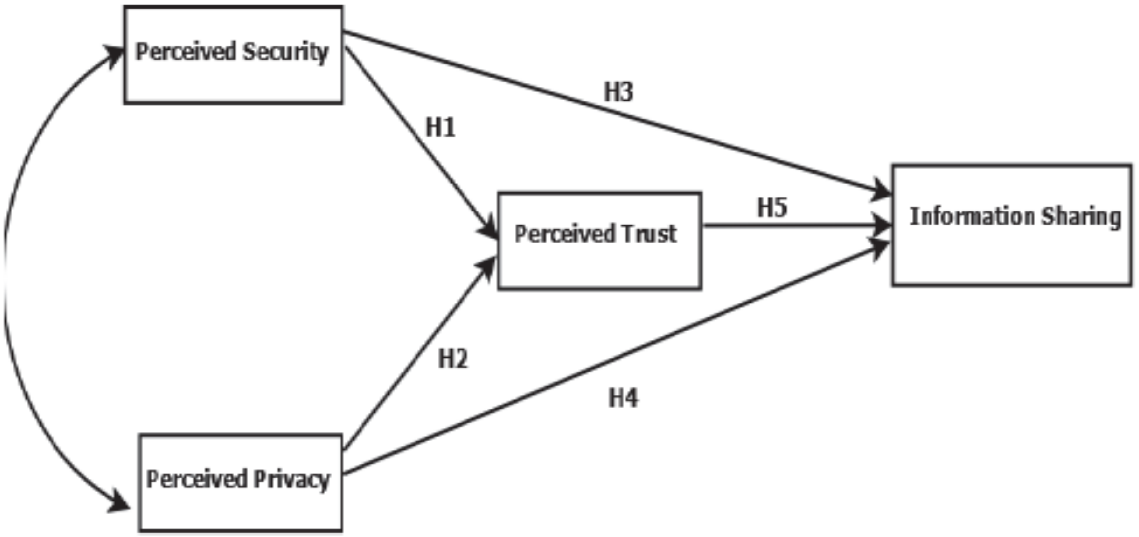
1) The first investigated article is “A Model of Unwanted Leakage of Personal Information in Multiple Social Networks “. The authors are looking for ways to protect users' privacy and to reduce information leakage in the social network.
2) The second article, "The Success of Related Security in the Geography of Social Networks", in this paper, the authors examine four aspects of privacy related to position (No colleagues in

residence, protecting privacy in the geography of social networks, addressing potential attacks and protection techniques).

3) The third article is "Friend in the Attacks: Take Advantage of Social Networking Sites for Spam". Friend in the attacks can show herself as a social networking application in social networks and show how the enemy can use attacks to gather sensitive data.
4) The fourth paper is "Protecting Users' Privacy in the Communications of Online Social Networks". The authors classified available techniques for protecting the privacy of communications based on exposure to potential risks of users' identity [M.Shehab et al,2011].

3.5) Effect of trust, security and privacy concerns in social networks: An exploratory study to understand the pattern of disclosing information in Facebook

This study aims to develop a researching model with privacy and security concerns. The aim of the study is to understand the impact of security. In this article, an online survey has been used, and experimental data are collected from 250 Facebook users from different age groups and during the period of four months. The findings from the paper: the privacy concerns of respondents are based on significant statistics and suggests that privacy concerns such as security and trust effects positively on information sharing. This article has paid attention to the areas of privacy (in fact, it has used previous researches about security concerns in the social networking sites). In this article, a framework is shown to find the willingness to share information. The experimental hypothesis has been tested, and based on the hypothesis proposed in Figure 3: perceiving security, perceiving privacy and perceiving trust are influential factors for user's willingness in information sharing.



3. Proposed Hypothesis

In Table 4, an explanation of the relationship is stated (perceived security, perceived trust, perceived privacy, information sharing). In this section, a study was done to probe the efficacy of the proposed hypothesis. To do the study, a questionnaire was prepared within the framework of the proposed hypothesis and given to the number of users in Facebook. Details of these members are given in Table 5.

3. Explanations Of The Proposed Hypothesis

H#	Hypothesis
H1	Perceived security is positively related to perceived trust with in social networking sites.
H2	Perceived privacy is positively related to perceived trust with in social networking sites.
H3	Perceived security is positively related to information sharing in social networking sites.
H4	Perceived privacy is positively related to information sharing in social networking sites.
H5	Perceived trust is positively related to information sharing in social networking sites.

5. Characteristics Of Respondents To The Proposed Hypothesis

Profile	Items	Frequencies	Percentage
Gender	Male	189	77.1%
	Female	56	22.9%
Age	16-25 years	194	79.2%
	26-35 years	40	16.3%
	36-50 years	8	3.3%
Educational Qualification	Intermediate	23	9.4%
	Graduate	119	48.6%
	postgraduate	100	40.0%
Occupation	Student	165	67.3%
	Govt. Sector	43	17.6%
	Private Sector	14	5.7%
	Professional	18	7.3%

In the Table 6, the final results of the investigation about the proposed framework were classified by preparing a questionnaire. The main objective of this study was to assess the effect of user privacy concerns in client behavior as well as information sharing in social networks referring to Facebook [A.Dhami et al , 2012].

6. Results of Proposed Hypothesis

Hypothesis	Path coefficient	P-value	Support
H1:Perceived Security→ perceived Trust	**0.25****	**0.000**	**Yes**
H2:Perceived Privacy→ Perceived Trust	**0.51****	**0.000**	**Yes**
H3:Perceived Security→ Information Sharing	**0.22****	**0.000**	**Yes**
H4:Perceived Privacy→ Information Sharing	**0.04**	**0.500**	**No**
H5:Perceived Trust→ Information Sharing	**0.25****	**0.000**	**Yes**

4. Discussion

All above articles discussed challenges and security solutions in the OSN, but they are only part of the whole security story of OSN and the growth of these networks, and by increasing technology development, users' security in the network has become unsolvable problem, and everyday users are faced with a new serious threat approach. In the above articles, if the solution was also proposed by the article, no one did a very good and comprehensive solution. Each article is discussed or criticized in the following.

4.1 First paper. At first, It paid attention to social network and then to the security of networks, but it did not mention viruses, and malicious attacks and only it classified enemies in social networks and passed up the details of this important issue, but finally a solution was proposed that it could be used to progress in the field of social security in the future.

4.2 Second paper. This paper discussed a variety of attacks on social networks well, and it clarified the attacks very well, but just three cases were mentioned for defense mechanisms

in the client side, it also passed up discussing these cases, but in elsewhere, a defense mechanism on the server or the same social network was discussed and discussed the analysis or test solutions was passed up.

4.3 Third paper. First, this article paid attention to social networks, and then privacy in these networks. Three tools for the business of cybercriminals were mentioned in a part of this article. But the details of these tools were passed up, and no solution was mentioned to prevent them, only several recommendations were stated for users to improve their security, and no solution was suggested to increase security in social network sites.

4.4 Forth paper. This article addressed the problems of security in social networks through literature of other articles, it is a positive point because the used articles are rich, but it is also unfortunate that it did not review more articles, discuss more security issue, and criticize articles and that it just mentioned topic and a brief summary. But finally, it concluded on studies well.

4.5 Fifth paper. It is a good and complete article because at first it has examined security in social networks, then it has presented a framework to improve security in social networks for helping users, which has been tested and analyzed, and it has got a good respond from the tests, and no bad criticism can be mentioned for this paper except that this framework should be considered very well by client, and the framework can be violated if the client doesn't perceive each base of the framework.

5. Conclusion

Increasing use of social networks and sites, we are faced with a lot of vulnerabilities, one of the biggest which is users' lack of awareness about existing threats in the network and increasing the number of these networks. In this paper, we assessed several articles that had examined the security challenges in the network and ways to enhance the security of the networks have, and then we discussed and reviewed each of the papers and their pros and cones. Although all mentioned security issues were expressed very well in the articles, there are still more advanced security threats in the field of users' security in social networks. In the field of security in OSN, more researches should be done in the future, especially that most of these attacks is due to user's lack of awareness, and this is why we should consider not only servers but also users in all offered solutions. Todays, however there are many articles on this issue and solutions are provided, unfortunately we can see security breaches in the networks.

References:

A.Dhami. N.Agarwal. T.Chakraborty. B.Pratap Singh. J.Minj "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook" 978-1-4673-4529-3/12/$31.00_c 2012 IEEE

C .zhang J.sun X.zhu Y.Fang. "Privacy and Security for Online Social

G.Joon Ahn M.Shehab A.Squicciarini "Security and Privacy in Social Networks"

H.Gao. J.Hu. T.Huang. J.Wang. Y.Chen "Security Issues in Online Social Networks" Published by the IEEE Computer Society 1089-7801/11/$26.00 © 2011 IEEE

Networks: Challenges and Opportunities" IEEE Network • July/August 2010

Published by the IEEE Computer Society 1089-7801/11/$26.00 © 2011 IEEE

S.Abdulhamid. S.Ahmad. V.Waziri. F.Jibril "Privacy and National Security Issues in Social Networks " Challenges (September-December, 2011) pp 14 -20

www. Wikipedia.com.

www.hamshahriOnline.com