Sindh Univ. Res. Jour. (Sci. Ser.) Vol.43 (1-A) 109-114 (2011)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Social Applications: A Privacy Challenge for Online Social Networks

J. Ahmed[1], Z. A. Shaikh[1], S. Latif[2]

[1]National University of Computer and Emerging Sciences, Karachi, Pakistan
[2]Mehran University of Engineering and Technology, Jamshoro, Pakistan
zubair.shaikh@nu.edu.pk, engr_shiraz@ieee.org

Corresponding author: J. Ahmed shahani.javed@nu.edu.pk ,
rec

Abstract: Social networking sites are one of the most popular internet sites today. This is due to dramatic increase in the number of social networks users, which reached the 600 million users on Facebook alone as of March 2011. With introduction of the social networking platforms, third party developers are able to launch their own applications for existing massive user base. These applications can access user's profile data to operate properly. This fact poses serious privacy risks because current social networking platforms don't provide any mechanism to control disclosure of user's personal information to social applications and their developers. In this paper, we analyze usage pattern and growth rate of social applications. We present results of a research survey which was conducted at higher education institution. The results clearly demonstrate unawareness of user about privacy implications of using social applications. We also point out inherit flaws in existing social networking platforms. We recognize the need for extension of current social networking APIs so that these provide fine grain access control to the user of online social networks.

Keywords: Social Networking Sites, Social Applications, Privacy, Social networking APIs, Web 2.0

INTRODUCTION

Online Social Networks (OSN) such as Facebook, Twitter, LinkedIn, and Orkut has become immensely popular in the last few years. According to (Alexa, 2011) social networking sites are among top most visited sites in the world. The table 1 shows interesting facts about social networking sites popularity on basis of internet traffic generated across the globe and number of registered users. The rapid growth of these sites has raised many interesting and challenging problems for researchers working in this area. One of the challenging problems posed by OSN is privacy leakage of user's personal information. Users of social networking sites create profiles. These profiles contains vast amount of personal information about users. These users are also connected with other registered users of social networking sites. Controlling access to the information shared by users is a challenging task. In order to protect user's personal information, all social networking sites provide some level of privacy control. The most commonly needed privacy features are: profile privacy, application privacy and newsfeed privacy. However, privacy tools provided by social networking sites are not flexible enough to protect user data. In this paper, we will present privacy challenges posed by enormous usage of social applications.

Table. 1 Social Networking Sites Factsheet

Social Networking Sites	Ranking based on Global Internet raffic	Registered Users	Third Party developer's Platform
Facebook	2nd	500 million	Facebook API
Twitter	9th	106 million	Twitter API
LinkedIn	17th	100 million	Google's OpenSocial
Orkut	93rd	100 million	Google's OpenSocial

With emergence of Web 2.0 (Tim O'Reilly, 2005), social networking sites are offering open platforms to enable third party developers to develop applications which provide seamless integration of profile data to third party applications. Facebook, Google, and Twitter are leading this effort (Facebook, 2011) (OpenSocial, 2011) details about third party developer platforms supported by different ONS are given in **(Table 1)**. The Platforms provided by Facebook, Google, and Twitter opened doors for third party developers to launch their own applications for the social networking sites. These applications pose

serious privacy risk for online social network users because installed applications receives the privileges equal to owner of the profile and can access user's profile data. Facebook third party application developer policies (Facebook-TPA, 2011) clearly states that applications used by their users have access to their profile information to operate properly. Specifically, these applications have access to the public information of the users available in their profile and also to the information that users have made visible "for all" through privacy preferences of their profile. OSN Users are required to give full read permissions for profile information to the added applications (Irvine, 2008).

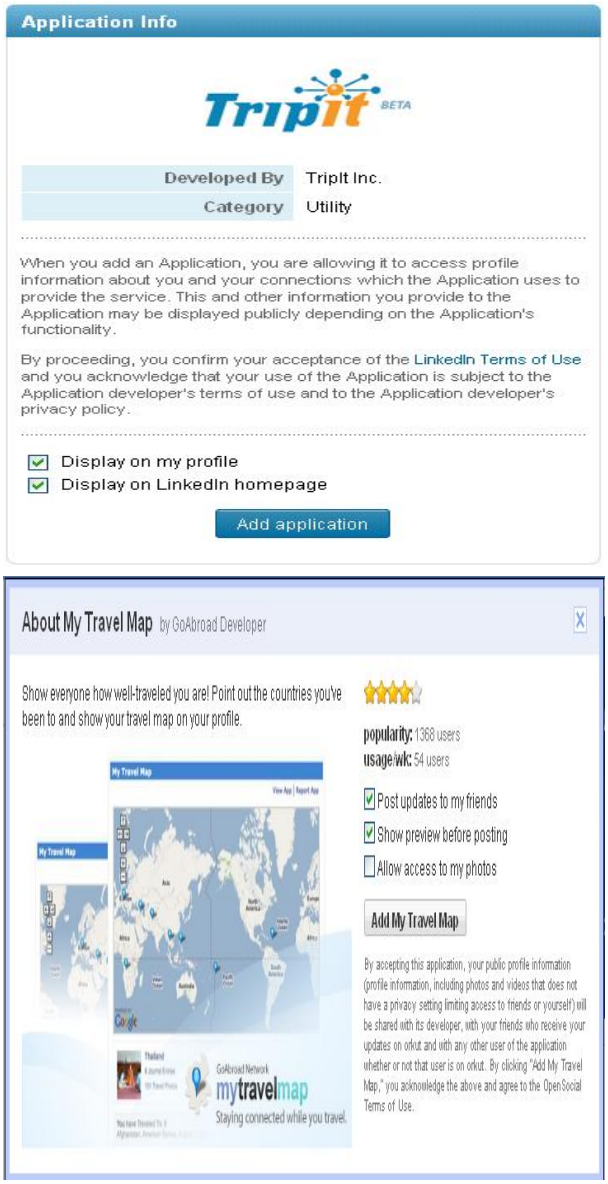

Fig. 1 LinkedIn and Orkut Application permission requests

The **(Fig. 1)** shows that Social application is added by user if and only if he/she grants full access to his profile, as well as to the profile data of his friends. If user doesn't agree to grant full access to the application being installed then process of installation fails. Third party application developers have access to user's data regardless of the actual application needs. OSN users are unaware of the amount of data being exposed to the external developers because such information flow is hidden or not clear to the users. This issue has been recognized by the media (Irvine, 2008) (Chris, 2008) (Jeffrey, 2008). In this paper, first of all we present results of research survey conducted about usage pattern of social applications and privacy perception of social application users. We also point out inherit flaws in existing social networking platforms which allow easy access of user profile information to third parties. We also point out limitations in existing solutions to the problem suggested by researcher community in the area. We recognize the need for extension of current social networking APIs so that these APIs provide fine grain access control to the user of online social networks.

The rest of the paper is organized as follows. Section 2 provides detailed literature review of the problem domain. In section 3, we provide detailed information about methodology used to determine the attitude of the users towards social networking sites and usage pattern of social applications. In section 4, we present results of the survey. In section 5 we discuss privacy implications of using social applications. The future work and conclusion is discussed in last section.

Literature Review

Privacy problem of social networking sites has been not only recognized, but also a huge amount of research work is done to counter the threats to profile information of OSN users. One of the first studies on privacy issues in OSN was conducted at Carnegie Mellon University in 2005 which analyzed 4,000 profiles of CMU students. As per the result of this research user of online social networks disclose huge amount of personal information in their profiles. Online social network users are less concerned to use site's privacy settings to control visibility of the profile; only 0.06% out of 4,000 users changed the default profile visibility in Facebook (Acquisti *et al.*, 2006). Most of the online social networks provide very permissive default settings and only very few users change their default settings as per the results of above mentioned research at CMU. Another research conducted by Ofcom after three years revealed that 48% of the participants reported that their profile was able to be seen only by their Friends (Ofcom, 2008).

According to (AiHo *et al.*, 2009) privacy tools in online social networks are not flexible enough to protect user profile data. Facebook is one of the few online social networks that provide granular access control mechanism. But current Facebook privacy interface is too complex therefore user's profiles are either entirely public or entirely private. Lipford *et al.*, proposes prototype for interface that help users manage privacy settings in more comfortable manner (Lipford *et al.*, 2008). However, privacy settings behind the prototype interface are almost the same. The prototype only slightly improves the user interface which help user to understand how privacy settings work.

Traditionally, most of the privacy research in online social networks is focused on protecting profile information of users from other users of online social network. For example, a user can be limited from seeing particular material or blocked entirely from seeing any material (Thomas *et al.*, 2010, Maximilien *et al.*, 2009 and Liu *et al.*, 2009). However, social applications have almost no such privacy controls. The amounts of users profile data accessed by social applications using APIs is uncontrollable (Renner, 2010).

The privacy risk associated with social networking APIs is addressed by (Felt *et al.*, 2008), this research analyzed 150 popular Facebook applications and showed that majority of the applications only need access to a user name, list of friends, and user's network information to function correctly. The authors also shown that as many as 91% of current social networking applications have unnecessary access to huge amount of data they do not need. The authors proposed a solution to these privacy risks that social networking platforms use privacy by proxy design. However, this approach does not work well with social applications using user's private data. (Besmer *et al.*, 2009) propose a new model for access control for applications on social networking sites. This model is highly dependent on the success of setting an appropriate user application policy which requires motivated users and there are several researches showing that online social networks user are less motivated to concentrate on setting their profile privacy. This research work does not provide any solution for privacy problem of social applications but point out inherit flaws in the design of existing social networking platforms and emphasize that privacy controls should be provided in APIs. This work also demonstrate lack of interest of OSN users towards privacy of their profile information, this hypothesis is supported by the results of a survey conducted about social application usage and profile privacy.

MATERIAL AND METHODS

Social applications are influencing the way content is being produced and consumed in OSN sites. These applications have viral growth features due to massive user base on social networking sites. It is necessary to conduct large scale measurement study of the usage patterns of social applications to gain better understanding of the potential threat involved in careless usage of these applications. We have compiled data from different web monitoring sites such as Alexa, to show usage patterns and growth rate of two mostly widely used sites around the globe. **(Table 2 and 3)** shows social applications usage statistics.

Table 2.Facebook Applications Usage Statistics

Applications	**Daily Active Users**	**Monthly Active users**
Cityvilla	7,233,791	118,378,432
Facebook for iPhones	38,333,135	69,835,909
FarmVilla	13,455,440	47,100,092
Texas HoldEm Poker	7,219,416	36,907,445
Facebook for Android	21,993,288	33,173,316
Mafia Wars Games	2,285,639	17,331,216
Causes	791,013	18,074,910
Birthday cards	549,877	9,079,761
Horoscopes	3,790,842	8,687,091
Events	167,453	7,018,018

Table 3. Twitter Application Usage Statistics

Applications	Monthly Unique Visits
TwitPic	1,236,828
Tweetdeck	285,864
Digsby	233,472
Twittercounter	212,200
Twitterfeed	149,812
Twitterholic	147,164
Twhirl	143,333
Twitturly	88,793
Twtpoll	74,154
Retweetist	60,051

These tables show tremendous growth in usage of social applications on Facebook and Twitter. In fact, Facebook and Twitter are no more just social networking site, but these are platforms which hosts thousands of third party applications. These applications gain access to profile data of millions of OSN users, those individuals are unaware of the ways in which their data is being used by third party developers.

The data presented in these tables clearly demonstrate the popularity of social applications and their phenomenal growth rate. It is also important to consider the awareness of users about kind of risk involved in providing huge amount of profile information to third party developers via social applications. So, we have also conducted a survey to know level of awareness users have about privacy implication of using social applications. This survey contained basic questions about the usage and privacy perception of users about social applications. Most of the participants of the survey are students and faculty of highly prestigious educational institution. All participants of survey had at least one social networking sites account.

RESULTS

As per the results of survey majority of participants added social applications to their profile. Most widely used type of social applications is utilities such as birthday calendar and games like FarmVilla.

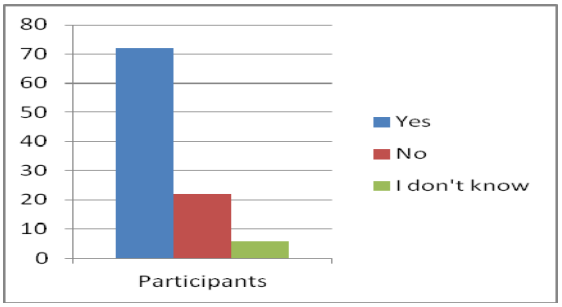

Fig. 2(a) Results about adding Facebook applications

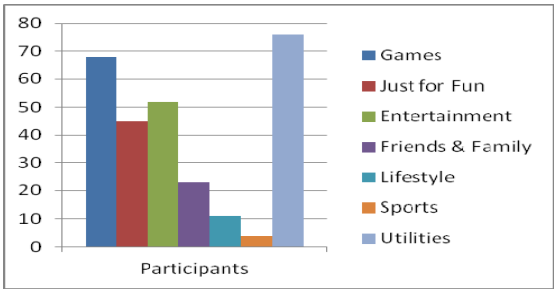

Fig. 2 (b) Result about type application used by participants

As per the results of survey majority of participants has perception that social applications does not have complete access to their profile data, whereas it has been clearly identified by (Felt et al., 2008) that 91% of the social application have full access to user profile data. In response to question regarding the privacy tools provided by social networking sites to control data access by social applications majority of users have perception that it is not provided, whereas 11% of users even don't know besides the fact that they have added social applications to their profile.

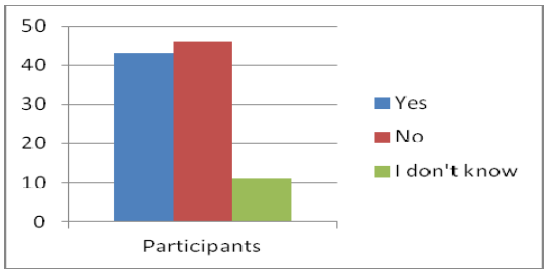

Fig. 3 (a) Results about privacy tool support by SNS

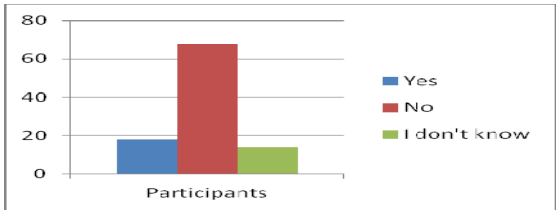

Fig. 3 (b) Result about profile data access by social apps

The result of the survey clearly indicates that vast majority of participants are unaware of second degree access by social applications. In response to question about social applications added by users can access profile data of his friends' more than 80% participant responded with negative answer, whereas Facebook provide second degree access to third party applications which means even if you don't add any social application to your profile but your profile data is vulnerable to privacy leakage due to your friends activities of adding social applications. One of the important questions to judge the privacy attitude of users was about reviewing the terms of service and policies before adding any social application. The result shows that vast majority of participants are less concerned about the privacy of their profile information.

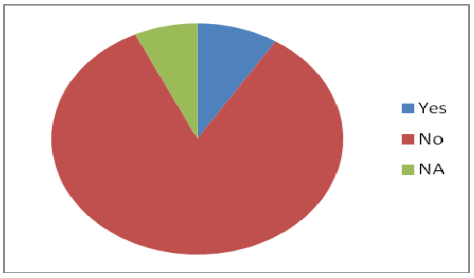

Fig. 4 (a) Results about reviewing terms and policies

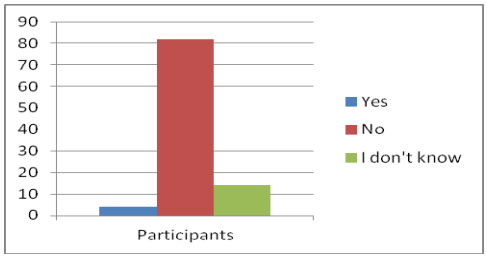

Fig. 4 (b) Results about second- degree access

The results of survey clearly demonstrate that attitude of SNS users towards their privacy is care free. They add social applications without reviewing terms and policies even they don't bother to protect their privacy using available privacy tools. They are unaware of the extent to which social application access their profile data and users also don't hesitate to harm their friend's privacy by allowing social applications to second degree access. It is very clear from the results of survey that users of social applications are unaware of the threat which is posed to their profile information by third party developers and their applications. In the next section, we discuss the possible privacy implication of using social applications.

DISCUSSIONS

Social applications transformed web into programmable platform which allow the creation of new applications made up of combinations of the data, functions, and user interfaces. These applications reuse sensitive data of OSN users which is clearer mirror of real life data. An important implication of this side effect is that users should pay careful attention to privacy capabilities and settings of social networking sites (Grandison *et al.,* 2008). Social networking sites don't provide any fine grain access control mechanism for controlling social applications. Basically, access control model adopted by social networking sites is an all or nothing policy (Shehab *et al.,* 2008). OSN users cannot explicitly choose their privacy preferences regarding social applications. They cannot specify to which information third party applications can access (Delgado *et al.,* 2010). This lack of control over third party applications increases the risk of having attractive applications that spy on users and collect their data. To demonstrate this risk, BBC News developed a malicious application that harvested vast amount of user profile data in just three hours (BBC News, 2011).

According to (Felt *et al.,* 2008), most of the social applications do not need the extensive user information which is provided to these applications. For example, "Send a Rose" application does not require unnecessary full access to the user's data. In fact, only 9.3% of Facebook applications require access to user's private data (Felt, *et al.,* 2008). Facebook additionally gives social applications second-degree access which means if Babar installs a social application then the application can also request information about Babar's friends and fellow network members. This gives an idea of the complexity of privacy configuration in social applications. When the complexity of task reaches certain threshold, then the task will be mostly ignored or set to default settings. Social networking platforms give third party developers access to user data that would not otherwise be available to the developers through the user interface of social networking sites. It is responsibility of social networking site to protect user data that has been entrusted to them. Displaying Term of Service (TOS) warning screen at the time user adds application is not sufficient, but social networking platforms need to provide privacy controls in the APIs. As a matter of fact, OpenSocial and Facebook Developers Platforms were not designed with privacy in mind.

CONCLUSION AND FUTURE WORKS

In this paper, we have discussed privacy issues emerging due to the enormous growth in usage of social applications. We have also presented results of research survey which was conducted at higher education institution. All the participants of survey have accounts on more than one social networking site. The results of the survey clearly demonstrate unawareness of users about privacy implications of using social applications. We have also pointed out some of the loopholes in existing social networking platforms. We have focused our discussion on user-to-application privacy breach in online social networks. Social applications are offered by third party developers through social networking sites. These applications request access to profile information of users without specifying which information will be accessed and how that information will be used by the applications. Clearly, this shows that social applications can easily harvest huge amount of personal information of social network users. It has been observed that social networking platforms do not provide any fine grain access control mechanism to safeguard users' data. In order to resolve these privacy problems, we have proposed modifications to existing specifications of social networking platforms so that these APIs support privacy controls. These privacy controls will provide application developers useful means to give online social network users more control over their profile information sharing with social applications. This paper also opens new lines of research for the researcher community working in the area of online social networks that how privacy could be integrated into current social networking platforms. However, current online social network structure does not preserve users' privacy from the beginning, so what we consider more relevant for the future research in the area is that an online social network should be implemented based on the privacy-by-design principles. In future we intend to develop extension for existing APIs so that this extended version gives more control to users to manage their profile information on fine grain level.

ACKNOWLEDGEMENT

This work has been supported by Higher Education Commission (HEC), Pakistan through the Indigenous PhD Scholarship. It is worth mentioning that this work is extension of my research work on comparative study of social networking platforms in which we have analyzed Facebook developer's platform and OpenSocial.

REFERENCES

Acquisti, A. and R. Gross (2006) "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook", Proceedings of the 6th workshop on Privacy Enhancing Technologies, 36-58.

Ai. H., A. Maiga, and E. Aimeur (2009) "Privacy Protection Issues in Social Networking Sites", Proceedings of the IEEE ACS International Conference, 271-278.

Alexa, A. (2011) "Top 5000 Global sites", http://www.alexa.com/topsites/

Besmer, A., H. R. Lipford, M. Shehab and G. Cheek (2009) "Social Applications: Exploring A More Secure Framework", Proceedings of the Symposium on Usable Privacy and Security, 1-10.

BBC News (2011) http://news.bbc.co.uk/2/hi/programmes/click_online/7375772.stm.

Chris, S. (2008) "Exclusive: Next Facebook privacy scandal", http://news.cnet.com/8301-13739_3-9854409-46.html

Delgado, J., E. Rodriguez, and S. Llorente (2010) "User's Privacy in applications provided through social networks", Proceedings of the ACM WSM10.

Felt, A., and D. Evan (2008) "Privacy Protection for Social Networking APIs", Proceedings of the Web 2.0 Security and Privacy.

Facebook (2011) "Factsheet", http://www.facebook.com/press/info.php?statistics/

Facebook-TPA (2011) "Third Party Applications" Developer Principles and Policies", http://developers.facebook.com/policy/

Grandison, T. and M. Maximilien (2008) "Towards Privacy Propagation in the Social Web.", Proceedings of the Web 2.0 Security and Privacy.

Irvine, M. (2008) "Social Networking Applications can pose security risk", http://www.pantagraph.Com/news/article_293a33e8-ec23-5cf3-9e9bd0cf07ec5475. html

Jeffrey R. (2008) "Study raises new privacy concerns about Facebook", http://chronicle.com/article/Study-Raises-New-Privacy-Co/465/

Liu, K. and E. Terzi, (2009) "A Framework for Computing the Privacy Scores of Users in Online Social Networks", Proceedings of the IEEE ICDM 09.

Lipford,H.R, A. Besmer, and J. watsonm (2008) "Understanding privacy settings in Facebook with an audience view", Proceedings of the UPSEC, 1-8.

Maximilien M. T. Grandison, T. Sun, D. Richardson, S. Guo, and K. Liu (2009) "Enabling Privacy as a Fundamental Construct for Social Networks", Proceedings of the IEEE conference on Social Computing.

Ofcom (2008) "Social Networking: A quantities and qualitative research report into attitudes, behaviors, and use", Office of Communication of United Kingdom.

Open Social (2011) "The Web better when it's social", http://code.google.com/apis/opensocial/

Renner, C. (2010) "Privacy in Online Social Networks", Master thesis, ETH Zurich, 2010.

Shehab, M. A. Cinzia, and G.J. Ahn (2008) "Beyond User-to-User Access Control for online Social Networks", Proceedings of the ICICS, LNCS 5308, 174-189.

Thomas D., C. Renner, T. Grandison, and M. Maximilien (2010) "Making Privacy a fundamental Component of Web Resources", Proceedings of the W3C workshop on Privacy for Adv. Web APIs.

Tim O' Reilly (2005) "O" Reilly Networks: What is Web 2.0.", http://www.oreilly.com/