Social Privacy Protector - Protecting Users' Privacy in Social Networks

Michael Fire, Dima Kagan, Aviad Elishar, and Yuval Elovici
Telekom Innovation Laboratories and Information Systems Engineering Department,
Ben-Gurion University of the Negev, Beer-Sheva, Israel
Email: {mickyfi,kagandi,aviade, elovici}@bgu.ac.il

***Abstract*—In recent years, online social networks have grown exponentially, as these networks are fantastic places to meet and network with people who share similar personal interests. Facebook, currently the largest social network, has more than 901 million active users. The amount of personal information each user exposes on social networks like Facebook is staggering. Recent research in the area of social networking evaluated that many Facebook users exposed personal information. Due to the many security concerns regarding online personal exposure, we developed the Social Privacy Protector, a software which aims to improve the security and privacy of Facebook users. The software contains three protection layers which improve user privacy by implementing different methods. The software first identifies a user's friends who might pose a threat, and then restricts this "friend"'s exposure to the user's personal information. The second layer is an expansion of Facebook's basic privacy settings based on different types of social network usage profiles. The third layer alerts the user about the number of installed applications on their Facebook profile which have access to their private information. An initial version of the Social Privacy Protection software was evaluated on 74 Facebook users and successfully assisted them in restricting the access of 392 friends.**

Keywords-Social Network Analysis; Social Network Privacy; Social Network Security; Facebook Application; Fake Profiles.

I. INTRODUCTION

In recent years, online social networks have grown rapidly and today offer individuals endless possibilities for publicly expressing themselves, communicating with friends, and sharing information with people across the world. A recent survey [1] estimated that 65% of adult internet users use online social networks sites, such as Twitter [2], LinkedIn [3] Google+ [4], and Facebook [5]. As of June 2012, the Facebook social network, has more 955 million monthly active users [6]. On average, Facebook users have 138 friends and upload more than 300 million pictures each day [6]. Moreover, according to the Nielsen "Social Media Report" [7], American internet users spent more than 53.5 billion minutes on Facebook in the month of May 2011, making Facebook the leading web-brand in United-States.

Due to the friendly nature of Facebook, users tend to disclose many personal details about themselves and about their connections. These details can include date of birth, personal pictures, work place, email address, high school name, relationship statuses, and even phone numbers. Moreover, Bosmaf et al. [8] discovered that an average of 80% of studied Facebook users accepted friend requests from people they do not know if they share more than 11 mutual friends. In many cases, accepting friend request from strangers may result in exposure of a user's personal information to third parties. In addition, personal information of Facebook users can be exposed to third party Facebook applications [9]. Another privacy concern deals with existing privacy settings which, for the majority of Facebook users, do not match security expectations [10]. This results in many users accidently or unknowingly publishing private information, leaving them more exposed than they assumed.

If a user's personal information is disclosed to a malicious third party, it can be used to threaten the well-being of the user both online and in the real world. For example, a malicious user can use the gained personal information and send customized spam messages to the user in an attempt to lure such users onto malicious websites [11] or blackmail them into transferring money to the attacker's account [12]. In order to cover their tracks, social network attackers can use fake profiles. In fact, the number of fake profiles on Facebook can be counted in the tens of millions. Facebook estimates that around 5%-6% of its users could be false or duplicate accounts [13].

In this paper, we present an application for protecting user privacy on Facebook. Our application provides Facebook users with three different layers of protection. The first layer enables Facebook users an easy method for controlling their profile privacy settings by simply choosing the most suitable profile privacy settings in just one click. The second layer notifies the user of the number of applications installed on their profile that may impose a threat to their privacy. The third layer analyzes the user's friends list to identify which friends of the user are suspected as fake profiles and therefore impose a threat on a user's privacy. The application presents a convenient method for restricting the access of these fake profiles to the user's personal information without removing them from the user's friends list.

The remainder of this paper is organized as follows. In Section II, we give a brief overview of various related solutions which better help protect the security and privacy of social network users. In Section III, we describe the Social Privacy Protector software architecture in detail. In Section IV, we describe the initial evaluation results. Finally, in Section V, we present our conclusions from this study and

 ISBN: 978-1-61208-228-8

offer future research directions.

II. Related Work

In recent years, due to the increasing number of privacy and security threats on online social networks users, social network operators, security companies, and academic researchers have proposed various solutions to increase the security and privacy of social network users.

Social network operators attempt to better protect their users by adding authentication processes to ensure that the registered user represents a real live person [14]. Many social network operators, like Facebook, also offer their users a configurable user privacy setting that enables users to secure their personal data from other users in the network [10], [15]. Additional protection may include defense against hackers, spammers, socialbots, identity cloning, phising, and many other threats. For example, Facebook users have an option to report other users in the network who harass others in the network [16].

Many commercial and open source products, such as Checkpoint's SocialGuard [17], Websense's Defensio [18], UnitedParents [19], RecalimPrivacy [20], and PrivAware application [21], offer online social network users tools for better protecting themselves. For example, the Websense's Defensio software aims to protect its users from spammers, adults content, and malicious scripts on Facebook.

In recent years, several published academic studies have proposed solutions for different social network threats. DeBarr and Wechsler [22] used the graph centrality measure to identify spammers. Wang [23] presented techniques to classify spammers on Twitter based on content and graph features. Stringhini et al. [11] presented a solution for detecting spammers in social networks by using "honeyprofiles". Egele et al. [9] presented PoX, an extension for Facebook which make all requests for private data explicit to the user. Anwar and Fong [24] presented the Reflective Policy Assessment tool which helps the user examine their profile from the viewpoint of another user in the network. Recently, Fire et al. [25] proposed a method for detecting fake profiles in online social network based on anomalies in the fake user's social structure.

In this study, we offer a method for protecting user privacy in online social networks by detecting users who may pose a threat to a user's privacy by restricting their access to the user's personal information.

III. Social Privacy Protector Architecture

To better protect the privacy of Facebook users, we have developed the *Social Privacy Protector* software (otherwise referred to as SPP). The SPP software consists of three main parts (see Figure 1) which work in synergy: a) *Friends Analyzer Facebook application* - which is responsible for identifying a user's friends who may pose a threat to the users privacy, b) *SPP Firefox Addon* - which analyzes the user's privacy setting and helps the user to improve their privacy settings in one click, and c) *HTTP Server* - which is responsible for the analyzing, storing, and caching software results for each user. In the remainder of this section, we describe in detail each individual SPP part.

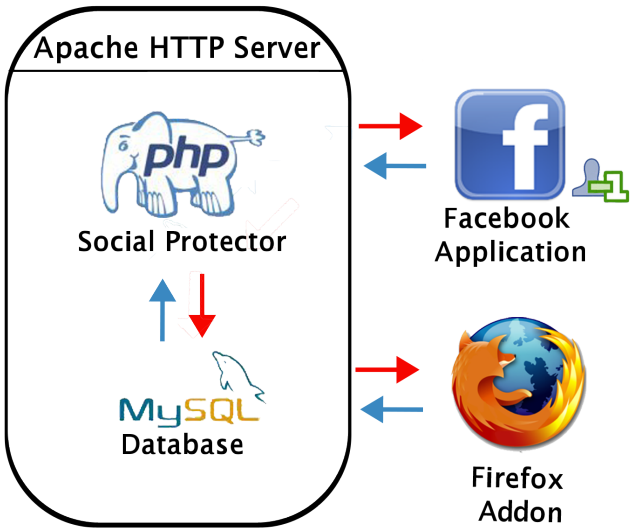

Figure 1. Social Privacy Protector Architecture

A. The Friends Analyzer Facebook Application

The Friends Analyzer Facebook application is the part of the SPP which is responsible for analyzing the user's friends list in order to determine which of the user's friends may pose a threat to the user's privacy. After the user installs the Friends Analyzer application, the application scans the user's friends list and returns a credibility score for each one of the user's friends. Each friend's score is created by simple heuristics which take into account the strength of the connection between the user and their friends. The application estimates the strength of each connection by calculating the number of common friends between the user and their friend, the number of pictures and videos the user and their friend were tagged in together, the number of groups the user and their friend were both members in, and the number of messages passed between the user and their friend. In the end of the process, the user receives a web page which includes a sorted list of all their friends. The list is sorted according to the score of each friend received where the friends with the lowest scores have the highest likelihood of being fake profiles appear on the top the list (see Figure 2). For each friend in the returned sorted list, the user has the ability to restrict the friend's access to the user's private information simply by clicking on the restrict button attached to each friend in the sorted list.

 ISBN: 978-1-61208-228-8

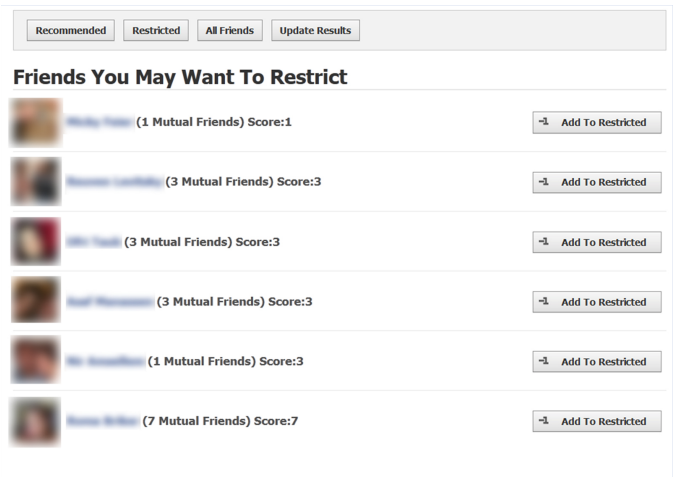

Figure 2. Friends Analyzer Facebook application - user's ranked and sorted friends list

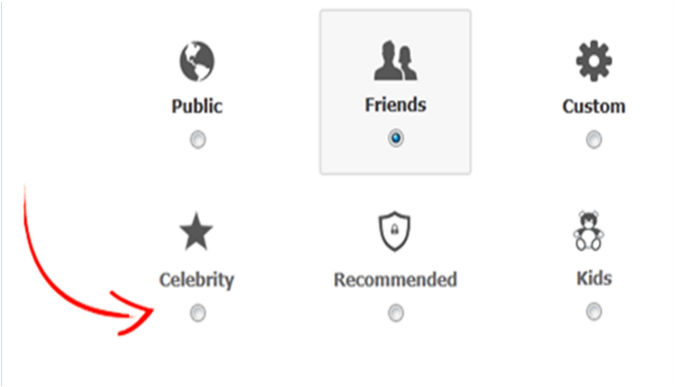

Figure 3. Social Privacy Protector Firefox Addon - optimizing the user's privacy setting in one simple click

B. Social Privacy Protector Firefox Addon

The Social Privacy Protector Firefox Addon (also referred to as Addon) is the part of the SPP software which is responsible for improving the user's privacy settings in just a few simple clicks. After the Addon is installed on the user's Firefox browser, it begins to monitor the user's internet activity. When the Addon identifies the user who has entered into their Facebook account, the Addon analyzes the number of applications installed on the user's Facebook profile and presents a warning with the number of installed applications that may pose threat to the user's privacy (see Figure 3).

The Addon also presents the top two results obtained by the Friends Analyzer Facebook application and suggests to the user which friends to restrict (see Figure 3).

The Addon also detects when the user has entered the Facebook's privacy settings page and presents the user with three new privacy setting options. The new privacy settings are based on the user's profile type and can be modified

Figure 4. Social Privacy Protector Firefox Addon - warning about installed applications and friends you may want to restrict

in one click (see Figure 4) instead of the more complex Facebook custom privacy setting that may contain more than 170 options [24]. Using the new Addon privacy setting, a user can simply chose the profile type most suitable for him out of three options: a) *Celebrity setting* - in this setting all of the user's information is public, b) *Recommended setting* - in this setting the user's privacy is only public to friends, however some of the user's details, such as profile name and pictures, are public, and c) *Kids settings* - in this setting the profile is only open to the user's friends and only friends of friends can apply for friend requests. Using this Addon, users can easily control and improve their privacy without the need to contact a security expert. Our application is also easy for customizing privacy settings by adding more privacy option settings to different types of users.

C. HTTP Server

The HTTP Server is the part of the SPP which is responsible for connecting between the SPP Firefox Addon and SPP Facebook application. Moreover, to enhance the application's performance, the HTTP server caches parts of the analyzed results. In order to protect the user's privacy, the application stores only the minimal number of features in an encrypted manner using RC4 encryption.

IV. Evaluation

An initial version of the SPP version was evaluated by 74 users who installed the Friends Analyzer Facebook application and 4 users who installed the Addon. Using the Friends Analyzer Facebook application, 31 users have a restriction of 392 ($median = 3$ and $\sigma_{dev} = 25.76$) friends. According to our initial evaluation results, the average common friends between the user and the friends they chose to restrict was

 ISBN: 978-1-61208-228-8

12.82 and the average number of common tagged pictures was 0.14 (see Table I).

Table I
FRIENDS AND RESTRICTED FRIENDS STATISTICS

Feature	Restricted Friends	All Friends
Common-Friends Average	12.82	32.32
Common-Groups	0.36	0.684
Tagged Pictures	0.14	1.39
Common-Messages	1.31	3.14

V. CONCLUSIONS AND FUTURE WORK

In this paper, we present the SPP software which aims to better protect user's privacy in Facebook. The software protects user's privacy by providing three layers of privacy protection. The first layer helps to restrict a user's friends access to personal information. The second layer help to identify and warn the user about installed Facebook applications which can violate the user's privacy. The third layer helps the user to adjust their privacy setting in one click. An initial version of the software was evaluated by 74 users and helped 31 users restrict the access of 392 friends to the users' personal information. As expected, in our preliminary results (see Table I), the application users' chose to restrict friends with less common features with them, such as number of common friends and number of tagged pictures.

The study presented in this paper is a work in progress with many available future directions. Using the SPP we can gather examples on which friends users tend to restrict. Using these examples, combined with Machine-Learning algorithms, we can improve the recommendation results on which friends to restrict. Moreover, in case many users restricted the same users, we can conclude with high likelihood that these users are fake users and recommend Facebook to remove them from the social network. Another possible future direction is to collect anonymous data on user privacy setting preferences. By using the users privacy preferences, we can create more types of "one click" privacy settings that serve other types of users and protect their privacy.

In the near future, we are going to release a final stable version of the SPP, and make it available to any user that want to improve his privacy on Facebook.

VI. AVAILABILITY

The Social Privacy Protector and parts of its source code are available for download from http://www.socialprotector.net. The Friend Analyzer Facebook application is available to download from https://apps.facebook.com/friend_analyzer_app. A video with detailed explanations on how to use the SPP application is available in http://www.youtube.com/watch?v=Uf0LQsP4sSs

VII. ACKNOWLEDGEMENT

We would want to thank Jennifer Brill for repeated readings and markups on our grammar and spelling. We also want to thank the anonymous reviewers for their valuable comments and suggestions to improve the manuscript.

REFERENCES

[1] M. Madden and K. Zickuhr, "65% of online adults use social networking sites," http://pewinternet.org/Reports/2011/Social-Networking-Sites.aspx.

[2] Twitter, http://www.twitter.com/, [Online; accessed 1-September-2012].

[3] LinkedIn, http://www.linkedin.com/, [Online; accessed 1-September-2012].

[4] Google+, https://plus.google.com/, [Online; accessed 1-September-2012].

[5] Facebook, http://www.facebook.com/, [Online; accessed 1-September-2012].

[6] Facebook-Newsroom, http://www.facebook.com, [Online; accessed 1-September-2012].

[7] Nielsen, "The social media report," http://blog.nielsen.com/nielsenwire/social/, [Online; accessed 1-September-2012].

[8] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The socialbot network: when bots socialize for fame and money," in *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM, 2011, pp. 93–102.

[9] M. Egele, A. Moser, C. Kruegel, and E. Kirda, "Pox: Protecting users from malicious facebook applications," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on*. IEEE, 2011, pp. 288–294.

[10] Y. Liu, K. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011, pp. 61–70.

[11] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM, 2010, pp. 1–9.

[12] S. Nelson, J. Simek, and J. Foltin, "The legal implications of social networking," *Regent UL Rev.*, vol. 22, pp. 1–481, 2009.

[13] Facebook, http://www.sec.gov/Archives/edgar/data/1326801/000119312512101422/d287954ds1a.htm#toc287954_2.

[14] J. Kuzma, "Account creation security of social network sites," *International Journal of Applied Science and Technology*, vol. 1, no. 3, pp. 8–13, 2011.

 ISBN: 978-1-61208-228-8

[15] S. Mahmood and Y. Desmedt, "Poster: preliminary analysis of google+'s privacy," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 809–812.

[16] Facebook, "Report abuse or policy violations."

[17] ZoneAlarm, http://www.zonealarm.com/, [Online; accessed 1-September-2012].

[18] W. Defensio, http://www.defensio.com/, [Online; accessed 1-September-2012].

[19] UnitedParents, http://www.unitedparents.com/, [Online; accessed 1-September-2012].

[20] ReclaimPrivacy, http://http://www.reclaimprivacy.org//, [Online; accessed 1-September-2012].

[21] PrivAware, http://apps.facebook.com/privaware/, [Online; accessed 1-September-2012].

[22] D. DeBarr and H. Wechsler, "Using social network analysis for spam detection," *Advances in Social Computing*, pp. 62–69, 2010.

[23] A. Wang, "Don't follow me: Spam detection in twitter," in *Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on*. IEEE, 2010, pp. 1–10.

[24] M. Anwar and P. Fong, "A visualization tool for evaluating access control policies in facebook-style social network systems," 2012.

[25] M. Fire, G. Katz, and Y. Elovici, "Strangers intrusion detection - detecting spammers and fake profiles in social networks based on topology anomalies," 2012.

 ISBN: 978-1-61208-228-8