# Security is in the Eye of the Beholder: Security Perceptions and Challenges in Social Networks

Ioanna Dionysiou
*Department of Computer Science*
*University of Nicosia*
*Nicosia, Cyprus*
*dionysiou.i@unic.ac.cy*

***Abstract*—This paper discusses security as perceived by social networking participants. A conceptual security framework is presented that captures the security requirements that a user engaging in social networking activities may impose on other users, the social network provider, and a third-party user. We claim that even though the social network users seem to not value at the fullest extent the security that privacy that they are entitled, still the providers are responsible for supplying a secure infrastructure for user interactions that will protect users from security and privacy threats.**

***Keywords*-social networks; security; user perceptions**

## I. INTRODUCTION

Even though social networking emerged as organized virtual communities in the last few years, its drastically-growing popularity is undisputed. Social networking sites such as Facebook, Linkedin, myspace, orkut, and twitter attract millions of users everyday. Social networking has been quickly adapted by the young population as the newest online trend, while there are very strong indications of a rapid growth amongst older users as well. According to a recent Nielsen report, *"social network and blogging sites are now the fourth most popular activity on the Internet"* [1], with the amount spent on these sites increasing by 63%. The popularity of social networks lies on the simple fact that they accommodate the exchange and sharing of information in an easy and intuitive manner for social, professional, and educational purposes. They even replace or supplement communications in the real world by diminishing barriers on physical location and time. Social networks provide opportunities to connect with friends, use short postings to inform friends on whereabouts, share videos and news, establish business contacts, advertise products, and campaign for various causes (political, social, etc.).

Social networks are subject to all common security vulnerabilities of the web [10] with their users being in even greater risk due to the implicit trust that governs these virtual communities. For example, users may show skepticism when receiving an email message that encourages them to click on a link or open an attachment, which is actually a malicious worm. However, they will click on such a link if it came from one of their social network connections. Needless to say, the sites that suffer more from security attacks are the most popular ones, and this realization has prompted several public and private bodies in lowering their tolerance of social networking activity during business hours. Besides the security concerns, privacy concerns also exist in social networks due to the vast amount of data that gets collected by the providers, allowing them to become digital *big brothers*. Personal and professional data could be exploited for a number of purposes, ranging from harming the system itself to increasing economic profits via data mining techniques. As an indicator of the monetary value of the stored data, the value of Facebook has been estimated to approximately $15 Billion.

Social networking represents the next generation of the Internet. It is here to stay. The aim of this paper is to investigate the security and privacy risks when interacting with social networking sites and present a security framework that those risks could be systematically assessed. Prior this discussion, a compact introduction to the structure and functionality of social networks is presented. Next, the findings of an empirical study that investigated the user perceptions of social network security is discussed. Security challenges of the construction of a global social network constitute the concluding part of this work.

## II. SOCIAL NETWORKING SITES (SNSS) ESSENTIALS

According to [8], social networking sites (SNSs) are web services that allow users to manage their profile within a bounded system, establish a list of connections, and finally traverse their connections' lists. However, this definition does not address the creation of new content and its dissemination among participants, which is after all the driving force behind social activities, either online or offline. Thus, a complete definition is one that relies on the *functional triangle* of social software that defines social software in terms of both information exchange and relationships. To be more precise, there are three primary functions of social software [3]:

1) Information management: creation, dissemination, and management of content, including searching

 ISBN: 978-1-61208-200-4 

2) Self management: presentation of one's self to reflect various aspects of his/her personality
3) Relationship management: provision of profiles and management of connections

Hence, social networking sites are web services that support online social networks that provide to their members a platform that integrates a variety of information management and exchange tools (blogs, forums, instant messaging event management, media uploading applications, podcasts, etc.) as well as relationship management tools (profile construction, connection lists, searching). In addition, the SNS platform allows a user to express the aspects of him/herself that are considered to be important in the particular online community.

If we were to classify SNSs based on the type of information handled, then two categories arise: the first one is the group of SNSs that is used primarily for professional information dissemination, such as Linkedin that manages business contacts. The second group focuses on personal and private information and its character is more informal. Such an example is myspace.

A social network compromises of the SNS provider, the member users, and third-party sites that develop applications interacting with the SNS platform (e.g. in the case of Facebook). A user registers with the particular SNS and creates a profile by supplying basic, personal, contact and professional information, with an emphasis on the category that best represents the nature of social network. The user can use applications developed by the SNS providers or request use of a third-party application after getting authenticated by the SNS.

Facebook is selected from a plethora of social networks to serve as the example social network to demonstrate the functionality of a typical social networking site. The choice of Facebook is based on the undeniable fact that it is the largest and most feature-rich social network, with a rather broad set of privacy policies and thousands of third-party applications running on its platform. According to Jeff Rothschild, the Vice President of Technology at Facebook, there are currently 30000 servers supporting the operations of Facebook, with 25 terabytes of logging data managed daily on behalf of 300 million active users. Facebook develops its own in-house technologies to facilitate the sharing of information among its members, such as photos, notes, groups, events, posted items, video, marketplace, gifts. It supports features such as news feed, share, and wall for up-to-date info. The open Facebook API enables developers to integrate their own applications with Facebook and gain access to millions of users. However, the intriguing potentials of Facebook have an impact on the security and privacy of users, as it will be discussed later on.

## III. Security and Privacy Risks

*Security is in the eye of the beholder.* The 2011 review of social networking sites as posted on the *www.toptenreviews.com* clearly suggests that the security of the most popular social networks ranges from *very good* to *excellent*. The evaluation criteria to assess the security of those sites were the following: support of privacy settings, block user feature, report spam feature, report abuse feature, and finally provision of safety tips.

This perception of security gives uninformed users a false reassurance. As a matter of fact, social networking sites suffer from a number of security vulnerabilities that could be exploited intentionally and accidentally [7], [24]. Facebook has suffered already XSS exploits, in the form of session hijacking and fake login pages. The infamous *harmless* Samy XSS worm shut down myspace in 2005 despite the fact that it only created inconvenience by adding the words *samy is my hero* to the top of every affected user page. Orkut users fell victims of a twitter-based scam, when they were lured to download a fake flash update that resulted in the launch of the worm that started harvesting google account details. Myspace and Facebook users were also the targets of the Koobface.a and koobface.b worms respectively. When a user of an infected machine log in to their social networking sites, fabricated messages were posted to the user's friends encouraging them to visit the malicious page.

Security and privacy in social networks as perceived by the users is also being investigated [4], [13], [20], [21]. Users seem to expect from the social network providers to support:

- Trustworthy environment: the community members should be able to trust each other, including applications.
- Privacy: users should be in control of privacy settings, which must be flexible and extensible
- Identity: even though the users are encouraged to reveal as little as possible to protect themselves from malicious acts, anonymity should be revoked when user harassment takers place
- Access control: users should have control over the content they generate by deciding its dissemination and revocation at any given time.
- Transparency: users must be informed how the collected data is used

Interestingly enough, there was no mention on vital security issues such as data integrity and confidentiality. The security and privacy problems do not only lie in the presence of design and implementation faults; the users carry their share of responsibility as well. If we were to examine the weakest links in the security of social networking, the investigation should have focused on all three participants groups as their actions have an impact on the overall security of the system:

- Users: The user behavior and user unawareness re-

 ISBN: 978-1-61208-200-4 

grading security are the primary factors that often lead to security and privacy problems. Bad habits also constitute a large fraction of the problems [10], [9]. User connectivity has become the primary objective of a significant number of users, who judge their importance by the numbers of friends they have. Experimental studies [18] have shown that almost half of the users agreed to accept as a friend someone they did not know, especially if a mutual friend existed between the requester and the target user [17]. This careless behavior increases the risk of being the victim of an attack, as a user with hundreds of friends is more likely to be subject to security breaches. In addition, users feel shielded from outside harm in online communities because they completely trust their connections. That's why they are more likely to click on a malicious link sent by a friend than if the link was sent via email, or they are willing to share personal information online than they would not normally do offline.

- SNS Provider: The SNS providers do not educate the users of risks of disclosing personal information [12]. For instance, users cannot control what their friends can reveal about them when using the tagging feature of Facebook. In addition, privacy tools and settings are not flexible or they are too complicated to be used properly by the average user. SNS providers do not provide the necessary security provisions for a number of security services, as it will be discussed below.
- Third-party: Social networks are complex systems that have their content and functionality enhanced by third-party applications. Rigorous methods are required to assess the security of the these system, and still is an open problem how to evaluate the security and safety of modules composition. As s result, malicious third-party applications could be launched via Facebook.

## IV. User Perceptions of Security of Social Networks

In order to investigate the user perceptions of the security and privacy risks when interacting with social networks, a survey was conducted among Cypriot university students. The survey questionnaire (available upon request) focused on closed-ended questions that addressed factors involving most security services, such as authentication, confidentiality, integrity, access control, and privacy. It comprised of three sections. Part A collected demographic details, educational status, and internet usage information for the respondent. Part B aimed in gathering more information regarding the online activities a responded was involved in. Part C examined the perceptions that a social network user has on matters involving security risks, profile data disclosure, authentication process, privacy settings, privacy and confidentiality issues. At the end of the survey, the respondent was prompted to answer whether or not he/she will do anything different after taking the survey.

Questionnaires were collected during the period of October 2011 until December 2011, and the survey was conducted through personal interviews to assure the highest possible degree of accuracy for the received responses. The non-probability quota sampling method was employed with a sample of 109 users. The social network users were 86 and the non-users of social networks were 23. Starting with the findings for the first two parts of the survey, a total of 74% of the participants fell in the 18-34 age group, 86% of the respondents were listed as university students studied either in Cyprus or abroad, and 73% was using the internet on daily basis. Surprisingly, all social network users had a Facebook account, and approximately 10% also had a twitter account. It seems that Facebook is the dominant social networking site among Cypriot university students. When it comes to ways of accessing the social networking site, the most popular mean was using a laptop(45%), followed by a desktop (33%), and then a mobile phone (18%). The remaining users made use of tablets or another device.

The majority of the respondents claimed to be aware of social security risks in general (68.6%), however it is alarming that 15.1% is not aware of such risks and a percentage of 16.2% does not even know what a security risk is. As a follow up question, 32.5% responded positively when asked if they use a public machine to logon in a networking site and do not uncheck the *"keep me logged in"* button. Furthermore, 41.8% use the same password to log on to various social networking sites.

Figure 1 shows the response distribution for the questions referring to profile information and Figure 2 lists the responses for the profile settings. 6.9% of the users post their cell phone number on their public profile that is viewable at least by their connections and/or strangers. Approximately 40% of the respondents are not aware who can view their profile and are not concerned who has access to their information. A percentage of 36% is aware of the information that third-party applications collect, and a 27.9% even claims to know how the information is used and stored by such applications.

| Question | Yes(%) | No(%) | I do not know(%) |
|---|---|---|---|
| Do you block your profile from public searches? | 48.8 | 13.9 | 37.2 |
| Do you have your birthday on your profile? | 80.2 | 13.9 | 5.8 |
| Do you have your hometown on your profile? | 70.9 | 23.2 | 5.8 |
| Do you have your cell phone number on your profile? | 6.9 | 84.9 | 8.1 |
| Do you know who can see your profile? | 61.6 | 16.2 | 22.1 |
| Do you know that you can see a preview of your profile when people look for you? | 59.3 | 17.4 | 23.2 |

Figure 1. Response Distribution for Profile Question Set

Figure 3 shows the response distribution for questions

| Question | Yes(%) | No(%) | I do not know(%) |
|---|---|---|---|
| Did you ever change any of those settings? | 62.8 | 19.7 | 17.4 |
| Do you find the settings too complicated or too time consuming to change? | 13.9 | 59.3 | 26.7 |
| Do you know what information a third party application (e.g. game) wants to access in order to use the application? | 36.0 | 24.4 | 39.5 |
| Do you know where the information that the third party application collects is used\stored ? | 27.9 | 36.0 | 36.0 |
| Have you even denied access to your information when a third party application requested it? | 52.3 | 17.4 | 30.2 |
| Are you concerned if your information is shared with people you don't know? | 61.6 | 15.1 | 23.2 |

Figure 2. Response Distribution for Profile Settings Question Set

that involve a user's connections. An impressive 69.7% has accepted connection requests from strangers, showing that university students are willing to add into their circle users that they don't even know. Furthermore, 73.2% admitted that they click on a link posted by friends.

| Question | Yes(%) | No(%) | I do not know(%) |
|---|---|---|---|
| Have you ever accepted friend\connection requests from strangers? | 69.7 | 23.2 | 6.9 |
| Do you know who can view your posts? | 65.1 | 23.2 | 11.6 |
| Do you think that your posts may be viewed in the future by potential employers? | 50.0 | 15.1 | 34.9 |
| Have you ever click on a link posted on your wall by a friend? | 73.2 | 11.6 | 15.1 |

Figure 3. Response Distribution for Friends Question Set

Finally, Figure 4 reflects the replies of the respondents on privacy and other security risks. Less than half of the users have read the terms of service regarding the social networking site they are using. In addition, only half of them are aware of the information that the social network provider is collecting. Almost one fifth of the users believed that a third-party application is a legitimate application.

To conclude, it seems that not all users are concerned about privacy, access control of their information, storage or distribution of their personal data, confidentiality, and authentication. Besides, only 11.6% responded positively when asked if they will do anything different after taking the survey. This is an indication of lack of security-awareness among the target population, which is not always due to ignorance but it could be intentional as well.

## V. Security Framework

Even though the social network users seem to not value at the fullest extent the security that privacy that they are entitled, still the providers are responsible for supplying a secure infrastructure for user interactions that will protect users from security and privacy threats. To assess and evaluate the security model of a social network, a systematic approach is needed to define the security requirements and characterize the approaches to satisfy them [23]. For our purposes, the

| Question | Yes(%) | No(%) | I do not know(%) |
|---|---|---|---|
| Have you read the Statement of Rights and Responsibilities or Terms of Service, or any other relevant document regarding the social networking site you are using? | 38.4 | 47.7 | 13.9 |
| Do you know that Facebook receives data from the computer, mobile phone or other device you use to access Facebook? This may include your IP address, location, the type of browser you use, or the pages you visit. | 48.8 | 36.0 | 15.1 |
| Are you concerned about the following Facebook policy: «We only provide data to our advertising partners or customers after we have removed your name or any other personally identifying information from it, or have combined it with other people's data in a way that it is no longer associated with you.» | 44.2 | 30.2 | 25.6 |
| When you chat with a friend, are you concerned that someone else could view it? | 41.8 | 27.9 | 30.2 |
| When the third-party application requests access to your account, do you believe that this is a legitimate application? | 19.7 | 24.4 | 55.8 |
| Are you concerned with how all the material you post on the social network (photos, chats, posts, etc) are stored? | 47.7 | 17.4 | 34.9 |
| Will you use social networks for purchases? | 13.9 | 41.8 | 44.2 |
| Have you experienced a security incident in the social networking sites? E.g. virus, worm, cannot login because the site is unavailable | 30.2 | 44.2 | 25.6 |

Figure 4. Response Distribution for Security Risks Question Set

security services required by a social networking site are the standard security services as defined by X.800: user authentication, data integrity, data confidentiality, data availability, and access control. Privacy, the ability to hide personal information from the system, is also a required service due to the vast volumes of data collected by both the provider and third-parties. Table I illustrates the comprehensive security and privacy framework for social networking, where services are established with connection to the system participants. In the discussion below, the focus is on the user-oriented requirements. The requirements imposed on the user by the SNS or the third party are outside the scope of this discussion.

Table I
Security and Privacy Framework

| | user-user | user-SNS provider | user-Third Party |
|---|---|---|---|
| authentication | no | yes | no |
| integrity | yes? | yes? | yes? |
| confidentiality | no? | no? | no? |
| availability | yes | yes | yes? |
| access control | yes? | no | yes? |
| privacy | yes? | no | yes? |

### A. Authentication

Authentication is one of the security services that is provided by almost all social networks. It refers to the assurance that the communicating entity (user, provider, third party) is the one that it claims to be. In order to

 ISBN: 978-1-61208-200-4 

implement the authentication service, credentials such as username (or email) and password need to be supplied by the unauthenticated user, and upon verification the user is either authorized to log on or access is not granted. In the case of Facebook, an SSL connection is established during the authentication phase so that the message exchange will be protected from eavesdropping. An authenticated user is presented with a session key that is used throughout the active session for any further authentication purposes.

When a user interacts with a third-party application, the authentication process will still be performed by the SNS provider. The third-party server does not perform any authentication on the user. Similarly, a user does not have the means to authenticate another user; there are no tools or mechanisms to verify the identity of another user. This is especially problematic when anonymity is viewed favorably by a number of users in order to protect their identity.

### B. Integrity

Integrity refers to the assurance that the data has not been altered during its transmission to its indented destination. Due to the proprietary nature of the majority of social networks and the non-disclosure of technical specifications of the built-in or third-party applications, it is nontrivial to assess whether or not data integrity is part of the security model of the system and accompanied applications. There have been no incidents of message alteration (even though message fabrication has been witnessed), thus it could be assumed that some sort of message authenticator is generated that verifies the authenticity of the message. Taking Facebook as the example, the traffic among the external participants is digitally signed; however there is no description of how messages of built-in chatting applications are authenticated.

### C. Confidentiality

When assessing the confidentiality strength of social systems, one needs to take into consideration the underlying purpose of these systems. The original goal was to facilitate various forms of communication among interacting parties. Secrecy was not a main concern, whereas access control and privacy were top priorities. But, with the increase of sophisticated attacks by knowledgeable hackers, confidentiality should also be of an equal concern. Currently, it is not clear how the network servers of the social networks interact with each other, and what security protocols are using.

Consider chatting applications. It is well-documented that the .Net Messenger Service allows unencrypted traffic, making the wiretapping of such conversation subtitle to both passive and active attacks. Facebook Chat was found to be subject to similar problems and has already started preparing a new interface which will be based on Jabber's XMPP (extensible messaging and presence protocol) that uses encryption to protect the secrecy of the communicated messages.

However, it may not be performance-wise to encrypt all traffic that goes through the social network. Trade-offs have to considered and perhaps the user could either opt-in or opt-out when it comes to encrypting communication sessions for different applications. Moreover, users could increase or increase the encryption strength, but with a monetary cost.

### D. Availability

Availability is a system property where resources will be accessible and usable upon demand by an authorized system entity. Social networks suffer availability of service when denial of service attacks are launched due to either implementation vulnerabilities that get exploited or infected users that are used as points of launching worms and trojan viruses. Users expect their public profile information to be available to other users according to their preferences and they also anticipate that all features will be available whenever they want to use them. Users have the same availability demands from third-party applications as well – however, there are not any imposed availability requirements on the later applications. Needless to say, the more unavailable they are, the more users will abandon using their applications.

### E. Access Control and Privacy

Social networks emphasize access control and privacy as the two most important pillars of their security model. Users have strong expectations for privacy on social networking sites and they believe that it is the responsibility of the SNS providers to protect personal and user-generated content.

The two terms are often used interchangeably as they are both associated with restricting access to user data. However, privacy involves more than controlling who can access what; it allows a user to be part of the environment without leaving any traces and enables his/her easy and permanent withdrawal without any evidence of the prior interactions. It can be claimed that the design of social networks partially implements both privacy and access control.

Starting with the user-to-user access control, social networks offer profile "privacy", meaning that the user configures privacy settings that explicitly specify the group of users that are granted access permission to various profile properties. This is a course-grained access control that handles a limited number of access groups such as friends and everybody. However, there is the option to block users. Once the data is accessible by others, the owner of the data has no control over its further dissemination and usage. As far as privacy is concerned, social networks such as linkedin and facebook support the search feature that control who can search for the user and the ways to get in contact.

Third-party applications are granted second-degree access permissions, resulting in gaining access not only to the data of the user who authorized the application but also getting

 ISBN: 978-1-61208-200-4 

access to friends' data. In a sense, applications become automatically friends of the user. The application developers are obliged, as dictated by the Terms of Service, to display a warning screen asking the user's consent in accessing data; this is quite meaningless as the user is given no choice to restrict access to information that the application does not need or provide anonymized data. Once the application is authorized by the user, social network providers have no way to check how the information is used by the third-party application; they only have the developers' consent that they will observe the Terms of Service.

And when it comes to the SNS provider, there are no technical obstacles to prevent access to all user data, supplied and generated, and further manage it as the provider sees appropriate. It is important to note that the users volunteer to abandon their rights to privacy by agreeing with the Terms of Service. For instance, Facebook explicitly specifies that personal information is stored and web site information (browser type, IP address) is stored from the user's browser using persistent cookies. In addition, according to the Facebook Terms of Service there is a wide range of information that Facebook gathers about a user*"...We receive data about you whenever you interact with Facebook, such as when you look at another person's profile, send someone a message, search for a friend or a Page, click on an ad, or purchase Facebook Credits...We receive data from the computer, mobile phone or other device you use to access Facebook. This may include your IP address, location, the type of browser you use, or the pages you visit...When we get your GPS location, we put it together with other location information we have about you (like your current city). But we only keep it until it is no longer useful to provide you services."*. In other words, whatever a user posts, views, searches, exchanges is stored on the Facebook servers.

## VI. Social Network Challenges

The evolution of social networks into applications that span the web with millions of users plugged in offers new opportunities and challenges in the technological, economic, and social arenas. Below is a list (note: this list is by no means exhaustive) of security and privacy issues in each of these directions that are anticipated to be addressed in the near future.

### A. Technological Directions: Global Social Ecosystem

One of the technological challenges in building a social ecosystem is how to achieve interoperability among SNSs. Blosser and Zhan [6] explain that in order to build a collaborative social network, three main issues have to be addressed, one of them being how to combine the data of the various social network providers while preserving user privacy and provider confidentiality. OpenSocial [16][15] is a framework that interlinks social networks that support its API. However, there is no mention on how security and privacy are implemented in this network of social networks.

The second challenge focuses on the sociological aspect of a global social network [19]. Aggregating audience of different communities implies the merging of multiple identities that users may have in those communities. However, the ability of a user to have different identities and portray the self to other in various ways will be simply disabled by the interconnection of social networks. There must be ways to protect the various roles and data of a user in this interconnected network: the professional role and the social role must be clearly distinguished as they are in real life.

### B. Economic Directions

It has been observed that people tend to share the same interests with their friends, and this feature of *homophily* is vital if social networks were to be used for advertising. Various aspects of online advertising in social networks have been the subject of research works that present findings on how relevant online relationships are to advertising. The goal is to match an ad to a user. A recent study by Bagherjeiran and Parekh [5] investigated whether or not social network links are relevant to the targeted ads and how social information could be used in targeting methods to predict user response rates. It has been shown that the response rate on ads is indeed proportional to the number of connections who have responded in the past. They have hinted that relevant advertising will be more effective than viral spam.

The advertising business is already seeking ways to partner with social networks and gain access to the vast number of users that could be the target audience for their advertisements [2]. Mining social networks for viral marketing will be the future of advertising [22], with serious implications on the privacy of the user data.

### C. Social Impacts

Web-based social networking is also transforming social habits, especially of the youth, by shifting from face-to-face communication to online interactions. It is argued that social networking fulfills a human need, that of gossiping. The largest the size of your friends group, the more efficient the dissemination of gossip becomes. However, is this an evolutionary shift that will change the way we operate or will it diminish as years go by?

## VII. Conclusions

The popularity of social networking still exhibits an exponential growth, despite well-known and documented privacy and security breaches. The harm that a user may experience depends on how much the user engages in social networking activities. Social networks are complex systems and it is expected to observe security vulnerabilities from time to time.

 ISBN: 978-1-61208-200-4 

However, could it be the case that we are reaching a new era where perhaps there is no such a thing as privacy anymore? The ability to collect data and monitor activities has serious impact to the users' privacy. Third-party companies could correlate public profile data and sell their finding to credit-card rating companies, insurance companies, employers, etc. That brings the question of what happens next. Shall users become more alert regarding the consequences of their interactions? Should a code of etiquette together with violation consequences [22] be established as part of the terms of service? Should security be transparent to the user [14] or security preferences will be specified and observed via service-level agreements for fine-tune security and privacy based on the interaction [11]?

## REFERENCES


[1] *Global Faces and Networked Places: A Nielsen report on Social Networkings New Global Footprint*. The Nielsen Company, March 2009.

[2] Many online social networks leak personal information to tracking sites, new study shows, August 2009.

[3] Richter A. and Koch M. Social software - status quo, 2007.

[4] Esma Aimeur, Sebastien Gambs, and Ai Ho. Upp: User privacy policy for social networking sites. In *Internet and Web Applications and Services, International Conference on*, pages 267–272. IEEE Computer Society, 2009.

[5] Abraham Bagherjeiran and Rajesh Parekh. Combining behavioral and social network data for online advertising. In *ICDMW '08: Proceedings of the 2008 IEEE International Conference on Data Mining Workshops*, pages 837–846. IEEE Computer Society, 2008.

[6] Gary Blosser and Justin Zhan. Privacy preserving collaborative social network. In *2008 International Conference on Information Security and Assurance*. IEEE Computer Society, 2008.

[7] Joseph Bonneau, Jonathan Anderson, and George Danezis. Prying data out of a social network. In *2009 Advances in Social Network Analysis and Mining*, pages 33–40. IEEE Computer Society, 2009.

[8] D. M. Boyd and N. B. Ellison. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1):210–230, 2007.

[9] John Breslin and Stefan Decker. The future of social networks on the internet: The need for semantics. *IEEE Internet Computing*, 11(6):86–90, 2007.

[10] Steve Mansfield Devine. Anti-social networking: exploiting the trusting environment of web 2.0. *Network Security*, 2008(11):4–7, 2008.

[11] Ioanna Dionysiou, Dave Bakken, Carl Hauser, and Deborah Frincke. Formalizing end-to-end context-aware trust relationships in collaborative activities. In *International Conference on Security and Cryptography (SECRYPT08)*, pages 546–553, 2008.

[12] Ai Ho, Abdou Maiga, and Esma Aimeur. Privacy protection issues in social networking sites. In *ACS/IEEE International Conference on Computer Systems and Applications,*, pages 271–278. IEEE Computer Society, 2009.

[13] Amela Karahasanovic, Petter Bae Brandtzg, Jeroen Vanattenhoven, Bram Lievens, Karen Torben Nielsen, and Jo Pierson. Ensuring trust, privacy, and etiquette in web 2.0 applications. *Computer*, 42(6):42–49, 2009.

[14] Ryan Layfield, Bhavani Thuraisingham, Latifur Khan, Murat Kantarcioglu, and Jyothsna Rachapalli. Design and implementation of a secure social network system. In *IEEE Intelligence and Security Informatics 2009*, pages 236–247. IEEE, 2009.

[15] J. Mitchell-Wong, R. Kowalczyk, A. Roshelova, B. Joy, and H. Tsai. Opensocial: From social networks to social ecosystem. In *2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies*, pages 361–366. IEEE, 2007.

[16] Juliana Mitchell-Wong, Ryszard Kowalczyk, and Bao Quoc Vo. Social network profile and policy. In *2008 IEEE International Workshop on Policies for Distributed Systems and Networks*, pages 207–210, Los Alamitos, CA, USA, 2008. IEEE Computer Society.

[17] Frank Nagle and Lisa Singh. Can friends be trusted? exploring privacy in online social networks. In *2009 Advances in Social Network Analysis and Mining*, pages 312–315. IEEE Computer Society, 2009.

[18] Jan Nagy and Peter Pecho. Social networks security. In *Third International Conference on Emerging Security Information, Systems, and Technologies*, pages 321–325. IEEE Computer Society, 2009.

[19] Martin Pekarek and Stefanie Potzsch. A comparison of privacy issues in collaborative workspaces and social networks. *Identity in the Information Society*, pages 1–13, 2009.

[20] Cynthia Putnman and Beth Kolko. Getting online but still living offline: the complex relationship of technology adoption and in-person social networks. In *2009 Advances in Social Network Analysis and Mining*, pages 33–40. IEEE Computer Society, 2009.

[21] L. Sorensen and K.E. Skouby. Next generation social networks - elicitation of user requirements. In *IEEE 19th International Symposium on Personal, Indoor, and Mobile Radio Communications*, pages 1–5. IEEE, September 2008.

[22] Steffen Staab, Pedro Domingos, Peter Mika, Jennifer Golbeck, Li Ding, Tim Finin, Anupam Joshi, Andrzej Nowak, and Robin R. Vallacher. Social networks applied. *IEEE Intelligent Systems*, 20(1):80–93, 2009.

[23] William Stallings. *Network Security Essentials: Applications and Standards*. Pearson Prentice Hall, Upper Saddle River, NJ, USA, 3rd edition, 2006.

[24] M. Tubi, R. Puzis, and Y. Elovici. Deployment of dnids in social networks. In *2007 Intelligence and Security Informatics*, pages 59–65. IEEE, 2007.


 ISBN: 978-1-61208-200-4 