



Electronic Research Archive of Blekinge Institute of Technology
<http://www.bth.se/fou/>

This is an author produced version of a book chapter. The chapter has been peer-reviewed but may not include the final publisher proof-corrections or journal pagination.

Citation for the published chapter:

Title:

On the Concept of Trust in Online Social Networks

Author:

Henric Johnson, Niklas Lavesson, Haifeng Zhao, Shyhtsun Felix Wu

Book:

Trustworthy Internet

Year:

2011

Editor/s:

Luca Salgarelli, Giuseppe Bianchi, Nicola Blefari-Melazzi

ISBN:

978-8847018174

Pagination:

143-157

URL/DOI to the chapter/book:

10.1007/978-88-470-1818-1_11

The original publication is available at: www.springerlink.com.
Published with permission from:

On the Concept of Trust in Online Social Networks

Henric Johnson, Niklas Lavesson, Haifeng Zhao and Shyhtsun Felix Wu

Abstract Online Social Networks (OSNs), such as Facebook, Twitter, and Myspace, provide new and interesting ways to communicate, share, and meet on the Internet. On the one hand, these features have arguably made many of the OSNs quite popular among the general population but the growth of these networks has raised issues and concerns related to trust, privacy and security. On the other hand, some would argue that the true potential of OSNs has yet to be unleashed. The mainstream media have uncovered a rising number of potential and occurring problems, including: incomprehensible security settings, unlawful spreading of private or copyrighted information, the occurrence of threats and so on. We present a set of approaches designed to improve the trustworthiness of OSNs. Each approach is described and related to ongoing research projects and to views expressed about trust by surveyed OSN users. Finally, we present some interesting pointers to future work.

1 Introduction

Today the Internet has become an important world wide network that connects a tremendous amount of groups and people. These users are further exploiting the network in a way that its creators probably never imagined, with streaming applica-

H. Johnson
Blekinge Institute of Technology, 371 39 Karlskrona, Sweden, e-mail: Henric.Johnson@bth.se

N. Lavesson
Blekinge Institute of Technology, 371 39 Karlskrona, Sweden, e-mail: Niklas.Lavesson@bth.se

H. Zhao
University of California at Davis, 2109 Watershed Building, Davis, CA, 95616-5294, USA, e-mail: hfzhao@ucdavis.edu

S. F. Wu
University of California at Davis, 2109 Watershed Building, Davis, CA, 95616-5294, USA, e-mail: wu@cs.ucdavis.edu

tions, e-commerce, cloud computing, mobile devices and Online Social Networks (OSNs). Therefore, the Internet is feeling the strain and is struggling to deal with the ever increasing demands placed on it. However, what is great about the Internet is that anyone with an address on the network can contact anyone else who has one. But that is also what is terrible about it. Global connectivity (IP addresses and e-mail) means you have no way to prevent large-scale attacks, citing as an example recent digital assaults that have temporarily shut down popular sites such as Twitter. At the same time you are getting convenience, you are actually giving people the power to do damage [1].

In recent years we have seen a dramatic increase and a growing popularity of OSNs. An OSN consists of a virtual social graph where users (nodes) are connected with each other through a relationship, which forms the edges of the social graph. OSNs services for an individual are: (1) to create a public or semi public profile where they share personal information such as name, contact, interests (2) to establish a social circle of friends for information sharing and communication (3) to view and traverse friends' profiles and private information (4) to carry out real time and non-real time communication with friends in the form of comments, private messaging, chatting, picture tagging etc, and (5) to use a lot of third party applications that range from gaming to advanced communication, virtual gifts, event management, and so on [2]. The Internet, keeps on the tradition of providing different communication and information sharing services. OSNs represent a recent type of communication and socializing platform [3], which is highly welcomed by the Internet users. Unlike the traditional web which revolves around information, documents, and web items, the concept of OSNs revolve around individuals, their connections and common interest-based communities. Examples of popular OSNs are Facebook, Twitter and MySpace.

Although OSNs provide a lot of functionalities to their users, their enormous growth has raised several issues such as scalability, manageability, controllability, and privacy. OSNs give rise to trust and security threats over the Internet, more severely than before. Trust has been on the research agenda in several disciplines such as computer science, psychology, philosophy and sociology. The research results show that trust is subjective and varies among people. We believe that this subjectivity of trust has been overlooked in the design of OSNs. However, it is a complex task to mimic real human communication and transfer the real world relationships into the digital world. With the entrance of OSN, the Internet is beginning to look like a virtual society that copy many of the common characteristics of the physical societies in terms of forming and utilizing relationships. This relationship is unfortunately in current OSNs assumed to be a symmetric and binary relationship of equal value between the connected users and friends. In reality this assumption is wrong since a user has relationships of varying degrees.

The characteristics of trust can be defined as follows [4] [5]: *Trust is Asymmetric*: the trust level is not identical between two users. A may trust B, however, B may not necessarily trust A in the same way. *Trust can be transitive*: For instance, A and B know and trust each other very well, B has a friend named C in which A does not know. Since A knows B and trust B's friends, A might trust C to a certain

extent. Then C has a friend named D whom either A or B knows. A could then find it hard to trust D due to the fact that, as the link between friends grow longer the trust level decreases. *Trust is context dependent*: Depending on the context one may trust each other differently, i.e., trust is context specific [6]. *Trust is personalized*: Trust is a subjective decision and two persons can have different opinions about the trustworthiness of the same person.

The value of OSN is to form genuine relationships with people who are either acquaintances or strangers in real life and to generate social informatics from people's interaction, which not only benefits the social network communicators or cooperators, but also helps in finding business merits. However, to magnify the value of OSN is not an easy task. It is important to understand how to create an architecture for the social network itself such that its value can be protected and how to leverage the value of OSN in communication with social informatics techniques. Therefore, the research objectives should focus on establishing a trustworthy OSN environment to handle cyber security and privacy issues. In the long run, the use of social informatics can hopefully influence the future Internet or system design.

2 Background

The Internet introduces a powerful way for people to communicate and share information. However, in terms of security and trust there exist some serious problems. One problem is the Internet's anonymity, in which the network has no social context for either the message or the sender. Compare that with ordinary life; people generally know the individuals they are communicating with, or have some sort of connection through a friend. If the network could somehow be made aware of such social links, it might provide a new and powerful defense against different cyber attacks and, perhaps more importantly, increase the level of trust within OSNs. If a more fine-grained friendship level scale is introduced, some issues will be resolved, since the user can then specify an appropriate level of friendship depending on how much information he or she wants to share. However, this level could then be selected quite subjectively and perhaps even arbitrarily by the users, thereby reducing the potential for resolving the aforementioned privacy and integrity issues. Moreover, it is difficult to establish a meaningful scale for the level of friendship since it has to correspond to a variety of subjective beliefs about trust, integrity, and privacy.

In OSN, different friendship intensities have different levels of default trust, which should be reflected in the privacy settings. The typical user does not change their privacy settings that often. Therefore, the default setting should be appropriate in order to actually preserve privacy. Since users normally don't do it themselves, it would be nice to have an automated way of finding out about the intensity of the friendship and derive the privacy settings from the intensity value. Users do not only change the privacy settings often enough, but also the OSNs have not provided a distinction between the types of friendships, as every relation is a friend, regardless of how intense the relation is. It is, therefore, a need to automatically identify the

intensity of the friendship for the user. This way, the users' privacy settings could be reflective of the actual friendship intensity and automatically determined and set within the OSN for the specific user. This has to do with the relationship quality and an interesting approach to define the quality is to look at the interaction habits between users since it indicates differences in the strength of a relationship. This intuition is further discussed and supported in sociology research [7].

In social networks, individuals are connected with relations and these ties form the basis of their social network. These ties can in offline social networks (real life) be very diverse and complex depending on how close or intimate a subject perceives a relation to be. OSN, on the other hand, often reduces these connections to simplistic relations, in which you are friend or not [8]. These connections can be characterized by content, direction, and strength [9]. The intensity of a connection is also termed as the strength of that relationship. This characteristic indicates the closeness of two individuals or how powerfully two nodes are connected with each other in their social graph. Some users are prepared to indicate anyone as friends, while others stick to a more conservative plan. However most users tend to put other users on their list who they know or at least not actively dislike [8], i.e. this means that you can be friends in OSN even though the user does not even know or trust that person. This phenomenon is also very common in online social games, in which it is sometimes better to have as many friends as possible as a player. This could be a potential problem for social computing since OSNs might lose its value.

In offline social networks, the friendship intensity is a crucial factor for individuals while deciding the boundaries of their privacy. Moreover, this subjective feeling is quite efficiently utilized by human to decide various other privacy related aspects such as what to reveal and who to reveal. Therefore, in addition to other privacy and security threats, individuals can also face privacy threats from their own social network members due to the lack of trust and acquaintance. OSN users are unable to control these privacy vulnerabilities because: 1) Not enough privacy control settings are provided by OSNs, 2) The users do not know they have these settings, 3) The privacy controls are difficult to use, 4) Friendship is the only type of relationship provided by most OSNs to establish a connection between individuals, and 4) Individuals are unable to identify potential privacy leakage connections because their social networks consist of unreliable friends. Recently, some OSNs started to provide facilities to control information access but they are difficult to maneuver and normally overlooked by the users. Furthermore, the relationship status between individuals tends to grow or deteriorate with the passage of time. Therefore, these privacy settings once set, may become meaningless after sometime. The binary nature of a relationship makes privacy very uncontrollable for OSN users. In these circumstances, the estimation of friendship intensity is quite useful to identify internal privacy threats.

For OSN, we have seen an increment use and development of social computing applications. Most, if not all, of these applications handle the issue of trust in a very ad hoc way. OSNs such as Facebook provide a naive trust model for users and application developers alike, e.g., by default all your Facebook friends have equal rights to accessing the information such as profile, status update, wall post

and pictures related to a particular user. It is therefore of importance that application developers consider the trust and security issues within the scope of the application itself. Another interesting issue related to OSN is the ongoing data mining in which most OSN providers allow anybody to crawl their online data. The social computing paradigm has dramatically promoted the possibility to share social information online. Therefore, trust and security become increasingly challenging due to the speed and extent to which information is spread. On the other hand, how can this type of information sharing promote, e.g., the detection of malicious activity? The utilization of OSNs can further support authorities to handle crisis risk management and crisis management in a more efficient way. i.e., both by information dissemination and collection using OSNs.

While the popularity of OSN services, like Facebook and MySpace, are fast growing, some concerns related to OSN architecture design, such as privacy and usability, have emerged. For example:

- Friendships are not well differentiated. In reality, our friends can be classified with different circles, like families, colleagues, high school classmates, and etc. Furthermore, even in the same friend circle, we may stay closer to some people than the others. Even though current OSN services provide basic mechanism like friend list which provides more flexibility than before, it is still hard to differentiate the tie strength and the friendship quality and intensity between users.
- Personal information might be misused and privacy violation is also an issue of concern. Facebook provides various third-party applications that get access to personal information. Without surveillance and control on the applications they have joined, users personal information can be disclosed by malicious activity [10].
- All applications installed on Facebook use the same underlying social network, which is not only unnecessary, but also may result in privacy violation. Even if two users only want to cooperate or play together in just one application, they have to build friendship in Facebook. This may lead to unnecessary personal information disclosure.
- If a user posts something on his/her wall or someone else posts on the wall, all his/her friends granted with permission can see the post simultaneously. However, in real world, personal updates are spread asynchronously, probably from intimates to general friends. A similar asynchronous information spreading mechanism is also needed for OSN.

3 State-of-the-art

In general, trust can be defined as “The willingness of a party to be vulnerable to the actions of another part based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” [11]. In real life (face to face), trust is a critical determinant of sharing information and developing new relationships [12] [13]. Therefore, trust

should be an integrated concept in any network. There are in general two classes of trust systems [14]: a credit based system where the nodes are receiving credits and each message consumes a defined amount of credits [15]. The other part is reputation systems [16] [17]. The trustworthiness is then defined to be the probability that the next interaction is wanted. The reputation can be used on either a global scale with all other nodes or on a local scale for each neighbor.

An interesting project related to secured OSN is Safebook [18] that leverages the trust relationships that are part of the social network application itself. Safebook is a decentralized privacy preserving OSN that is governed by the aim of avoiding centralized control over the user data. The decentralization is provided by the use of peer-to-peer technology. The work presented in [19] describes a new application of threshold-based secret sharing in a distributed OSN. The developed mechanism will select the most reliable delegates based on an effective trust measure. Relationships between the involved friends are used to estimate the trustworthiness of a delegate.

A number of improved encryption solutions have been presented in the literature that are based on improved encryption and overall privacy management systems for OSN websites [20] [21]. Moreover, in a study conducted by C. Xi et al. [22], two different forms of private information leaks in social networks are discussed and several protection methods are reviewed. However, most of the current privacy improvement solutions add substantial amounts of user interface complexity or violate social manner. A good interface should not restrict or block users from contributing, sharing or expressing. Thus, a privacy preserving method within social norms is a difficult yet important research aim.

Gilbert and Karahalios [23] reflect upon the fact that social media treats all users the same: trusted friend or total stranger. In reality, Gilbert and Karahalios argue, relationships fall everywhere along this spectrum and in social science this topic has been investigated for a long time using the concept of tie strength. A quantitative experiment conducted in [23] shows that a predictive model that maps social media data to tie strength using a dataset of over 2,000 social media ties manages to distinguish between strong and weak ties with over 85% accuracy.

From a psychological or developmental point of view, a large amount of work has been conducted on establishing friendship measures, both for the real world and for the social media. For example, Punamaki et al. [24] study the relationship between information and communication technology and peer and parent relations while Selfhout et al. [25] focus on differentiating between the perceived, actual, and peer-rated similarity in personality, communication, and friendship intensity when two people get acquainted. Whereas Steinfield et al. [26] and Vaculik and Hudecek [27] investigate aspects, such as the building of self-esteem and the development of close relationships in a social network setting, Rybak et al. [28] try to establish a measure for friendship intensity in a real world setting. We believe that the OSN friendship concept could, and should, be more thoroughly investigated in order to improve the privacy and integrity of OSN users. Additionally, we argue that refined friendship level indicators, along with the content and interaction analysis required to develop these indicators, would enable the improvement of trust in OSNs.

As far as calculation of friendship intensity is concerned, an interesting study conducted by Banks et al is presented in [29]. They have introduced an interaction count method. In this method, they suggested to count selected interaction types between individuals in order to calculate the friendship strength. In addition to provide a novel intensity calculation method, they also suggested a framework that utilizes calculated friendship intensity for better privacy control in OSNs. In [30] the authors also utilized the number of interactions between individuals for the improvement of a recommendation process in OSNs.

To improve the current infrastructure defects of OSN, the Davis Social Link (DSL) research group¹ has developed an infrastructure: FAITH (Facebook Applications: Identifications Transformation & Hypervisor) to provide more trustworthy and flexible services to users. FAITH itself is a Facebook application, but works as a proxy between users and Facebook. It can hook other applications and provide services to the applications. Figure 1 describes the architecture of FAITH, in which FAITH provides three major functions:

1. Each application hooked under FAITH is monitored by FAITH. All Facebook Application Programming Interfaces (APIs) that the application called are logged and available for the user to review. The log information helps the users to keep track of their personal information executed by an application and also for the system to perform anomaly/intrusion detection.
2. Users can customize the API related to their personal information that an application can call. If a user feels an API is not necessary for an application, he/she can block the API so that the application can not access the user's relevant information. API customization prevents applications from maliciously impersonating the user.
3. Virtual social networks are generated and maintained for each application. FAITH initializes a friendship network for each application from Facebook. Users can then add or remove their friendships in an application hooked under Faith without affecting their friendships in Facebook. Similarly, they can also disconnect the friendships with others just within an application but not affect their friendships in Facebook. Virtual social networks provide users with flexibility to find new friendships and differentiate friend circles while protecting their privacy.

The DSL research group has developed several applications in FAITH to improve OSN user experience, boost communication and cooperation with social informatics techniques. There are two developed applications that we would like to highlight:

- SoEmail [31]: SoEmail stands for Social E-mail. Traditional email systems provide too little control to the recipient, so the recipient can not prevent from receiving spam. SoEmail incorporates social context to messages using an OSN's underlying social graph. If a sender wants to email a receiver, he/she should find a path on the social graph leading to the receiver. It mimics the real work social network. If two people are not friends and one wants to know the other, he/she need to find intermediate people with his/her social relationships to recommend

¹ <http://dsl.cs.ucdavis.edu/>

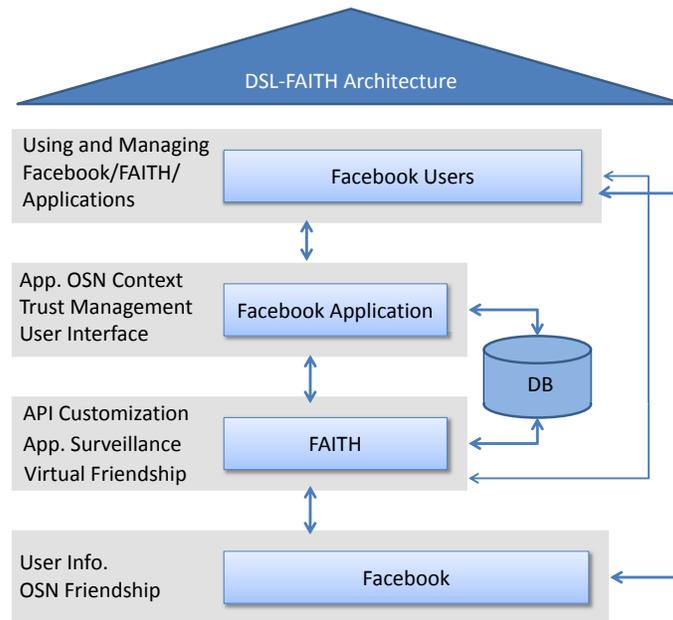


Fig. 1 The architecture of FAITH

him/her. If the receiver dislikes the email content, he/she can punish the social path from the sender, which decreases the trust value [32] from him/her to the sender.

- **SocialWiki [33]:** SocialWiki stands for social wiki systems. In current large wiki systems, a huge amount of administrative efforts are required to produce and maintain high quality pages with existing naive access control policies. SocialWiki leverages the power of social networks to automatically manage reputation and trust for wiki users based on the content they contribute and the ratings they receive. Although a SocialWiki page is visible to everyone, it can only be edited by a group of users who share similar interests and have a certain level of trust with each other. The editing privilege is then circulated among these users in an intelligent way to prevent spam. For a snapshot of SoEmail and SocialWiki see Figure 2.

4 Security Perception and Use of OSNs

It is quite evident that today's OSNs, such as Twitter, Facebook, Myspace, and Spotify, together represent a useful and exciting portfolio of ways to communicate and share information whether it be music, videos, news, or facts and fiction about ev-

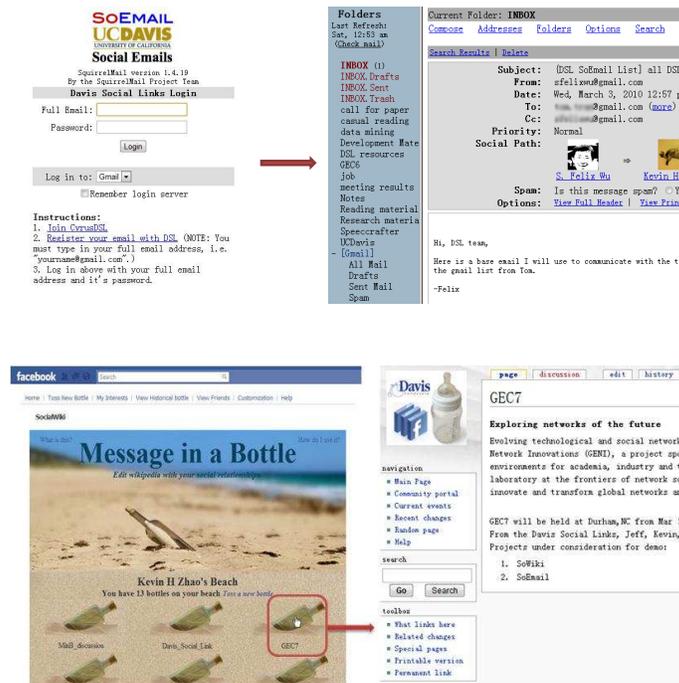


Fig. 2 SoEmail & SocialWiki

eryday life. Intuitively, the different OSN services emulate different parts of our lives and of the traditional ways we communicate and share information.

However, as can be observed in both scholarly literature and mainstream media, important concepts such as privacy, integrity, and trust, need to be redefined or at least considered using different approaches in OSNs compared to what is the norm in traditional social networks. Strong criticism has been raised against how privacy, trust, and security are implemented in the aforementioned OSNs. Perhaps most notably, there are countless cases in which the general population have published personal information in an OSN without really considering the consequences of making such content available on the Internet. For example, last year, the wife of the then new head of the British MI6 managed to cause a security breach and left his family exposed after publishing photographs and personal details on Facebook². In the aftermath of this and other similar events, the privacy concerns and online security awareness of OSN users have been frequently discussed.

Recently, an anonymous survey regarding OSN usage, addressing the problems of online privacy and trust, was conducted at Blekinge Institute of Technology [34]. The group of survey respondents consisted of 212 individuals from 20 nationalities. Out of the 212 respondents, 86% were male ($n = 182$) and 14% were female

² The Times, <http://www.timesonline.co.uk/tol/news/uk/article6639521.ece>

($n = 30$). The skewed male to female ratio is primarily due to the low number of female students at the School of Computing at which the survey was conducted. The participants were furthermore divided into three age groups; younger than 20, between 20 and 40, and older than 40. Quite intuitively, 96% of the participants belonged to the middle group (aged 20 to 40).

The aim of the survey was to gather information about the perception and use of OSNs, especially related to trust, privacy concerns, and integrity issues. In this particular survey, the scope was limited to Facebook users for several reasons: Facebook is one of largest and most well-known OSNs and, additionally, it has arguably been criticized heavily in both the mainstream media and in scientific work on the subject of lacking or too complex security and privacy settings.

A web-based survey questionnaire was created, which featured 21 closed questions. The questionnaire is logically divided into two parts: part one covers privacy-related aspects of Facebook usage and part two addresses the OSN interaction habits between the respondent and those users he or she considers as good friends. We will get back to the concept of good friends and its applicability to the enhancement of trust and privacy later.

As a basis for performing the analysis of the survey questions related to privacy and trust, the questionnaire featured a number of questions regarding the level of Internet experience as well as the frequency of Facebook usage. The results show that a majority of the respondents are active to very active Facebook users and most respondents regard themselves as being either expert or above average level Internet users. Thus, the survey results should be interpreted with this experience level of the respondents in mind. In other words, the results are hardly generalizable to the general population but should give an indication of what the thoughts and motivations of a large group of OSN users on the concepts of privacy and trust.

It is evident from the results of the survey that most users are connected to between 100 and 200 friends in the OSN. Almost 80% of the respondents have more than 50 friends in their network. A minority of the respondents have more than 1,000 friends in the OSN network. Naturally, if respondents were asked to estimate how many friends they have in their real world social network, it is plausible to assume that the number of friends would generally be much lower than what is observed in the OSN survey. However, in the real world social network, friends can usually be organized into groups of different levels of friendship (e.g., in terms of how long ago the friendship started or how active friends are in meeting and communicating with each other).

It is interesting to note that approximately 77% of the respondents are concerned about the privacy issues of Facebook and about 70% are actively avoiding to publish private data on Facebook due to privacy concerns. Judging by the frequency of alarms about OSN privacy breaches and issues, these figures either do not reflect the views and actions of the general population or it can be suspected that the media blows OSN privacy issue stories out of proportion for some reason.

A majority of the respondents (58%) are of the opinion that Facebook third party applications represent the biggest threat to privacy. The remaining respondents believe that their friends (16%) and friends of their friends (26%) pose a greater threat

to privacy. A quite staggering 66% of individuals suspect that at least one friend in their online network could have a malicious intent towards their privacy. It is also curious to observe that, 28% of those respondents who stated that their online friends could represent a privacy threat, report that they still add unknown people (e.g., people they do not know in the real-world) to their network. The willingness of individuals to expose private data to the friends they have in an OSN is arguably a factor that could reflect the confidence level the individuals attribute their friend network in the OSN. Close to 90% respondents only want to share their private data with selected friends in their network. In terms of general opinions regarding the security of the OSN, 56% of the respondents state that the Facebook privacy settings are too difficult to use. One interpretation of this result is that these users of Facebook are unsure whether the security settings they select really reflect their personal opinion on privacy and integrity.

5 User Interactions and their Implications

As has been previously discussed, the largest OSNs today, e.g., Facebook, employ a binary type of Friendship Intensity. That is, either two individuals have an established link as friends, e.g., a social link, or no direct link between them exists. From a privacy and integrity point of view, the binary friendship type poses several potential problems. For example, since users can only reject or accept a friend request (as no intermediate levels of friendship exist), there is a risk of unintentional sharing of personal information. The level of sharing is dictated by the OSN privacy settings, which many users neglect to get informed about or find it too time consuming and cognitively demanding to manually adjust. From the point of view of trust, we constantly assign different levels of trust toward our friends, relatives, business contacts, and so forth. The OSN binary level of friendship is not sufficient as a means to implement this real world concept of trust.

An important and open research question is whether (and how) the level of trust within OSNs can be increased by the use of social link content and friendship intensity determination. The average user seems to find it cumbersome to manually adjust privacy and security settings in the OSN. It would probably be even more difficult for users to manually establish the intensity of their relationship to other users. Thus, formulated more specifically, the question is how to reliably determine friendship intensity by automatic analysis of OSN user information and interaction data and how this can be used to better identify and determine social groups.

It is evident that technological advances have resulted in a general change of lifestyle and expanded the focus of the global economy from production of physical goods to manipulation of information [35]. As a consequence, we rely more and more on storing and retrieving information in/from databases. The number and size of the databases grow swiftly. It is even argued that stored data is doubling every nine months. It is therefore becoming increasingly hard to extract useful informa-

tion. It can be noted that data mining technologies have been shown to perform well at this task in a wide variety of science, business, and technology areas.

Data mining, or knowledge discovery, draws on work conducted in a variety of areas such as: machine learning, statistics, high performance computing, and artificial intelligence. The main problem studied is how to find useful information in large quantities, or otherwise complex types, of data. Although the nature of this problem can be very different across applications, one of the most common tasks is that of identifying structural patterns in data that can then be used to categorize the data into a distinct set of categories [35]. If these patterns can actually distinguish between different categories of data this implies that they have captured some generalized characteristics of each category. As it turns out, the area of machine learning provides a number of approaches to automatically learn this kind of concepts by generalizing from categorized data [35]. Moreover, regression problems, which have previously been studied in the statistics area of research, have also been revised and automated within the machine learning field. The question is whether data mining technologies, powered by machine learning theory, can be employed as a means to migrate the real world concept of trust to the OSN community.

A plausible approach for automatically determining friendship intensity would be that of establishing an appropriate friendship intensity model, based on Interaction Intensity [29], but with additional friendship aspects and by drawing on relevant work from both social science and information systems, e.g., [23] [24] [25] [26] [27] [28]. Such a friendship intensity model could be used as a basis for determining which user and interaction data to extract from the OSN, and for learning how to organize and preprocess these data, so that data mining algorithms can be applied to automatically predict friendship intensity. Thus, based on the friendship intensity model and the knowledge discovered through data mining, it would be possible to establish a new friendship intensity measure. This measure would of course have to be empirically compared to the state of the art using experimental evaluations on simulated and real-world data. A practical issue related to obtaining real-world data is that most OSNs (for example, Facebook) restricts the number of access attempts of user designed OSN applications. Thus, a quite elaborate batch-processing algorithm needs to be designed with deliberate restrictions concerning the number of accesses per some suitable time unit. Additionally, OSN friendship intensity may be defined as either a discrete or continuous metric, and the choice of metric type implies that either classification or regression learning algorithms are to be used for building the prediction model using the gathered data [35].

The data collection is believed to encompass a variety of data types such as text (e.g., personal descriptions, interests, observations, activities, and messages), numbers (e.g., years, months, and statistics like the number of sent and received messages), and categories (e.g., religious belief/political standpoint, events, locations). Thus, the learning algorithms selected for inclusion are required to handle these data types [35]. In the case where natural language is to be analyzed, the text needs to be transformed to an appropriate representation, such as the Bag-of-words model, which has been proven to work well for many text classification tasks, cf. [35].

6 Conclusions and Future Work

Although OSNs provide new and interesting functionalities that are very popular, the growth of these networks has raised issues related to trust and security. Examples of security concerns are that friendships are not well differentiated and personal information is unnecessarily disclosed and might be misused. If these issues are not prioritized the value of OSN might decrease. Therefore, the aim of our research is to establish a trustworthy OSN environment, in which the DSL research group has developed several novel applications that provide OSN users with flexible and secure services.

The results from a web-based survey questionnaire was presented that addressed the problem of online privacy and trust for OSNs. A majority (77%) of the respondent are concerned about the privacy issues and also of the opinion that third party applications are the biggest concern related to privacy. Most of the respondents also stated that the privacy settings on an OSN are normally too difficult to use.

The level of trust within a social network can in our opinion be increased by determine the friendship intensity. This is further discussed by the use of data mining to identify structural patterns in the interaction and non-interaction based data. One possible approach would be to establish an intensity model to determine different levels of friendship between your friends. In the future, we plan to develop a data mining framework and will utilize various classification and numerical prediction algorithms. Later on, we will validate the performance of this model on Facebook.

As part of future work, the DSL research group is continuously developing both FAITH and other applications. One feature in FAITH that is under development is Asynchronous Information Dissemination (AID). AID will be designed to increase users' flexibility to control the updates they want their friends to view. With AID, each user will be able to assign a rule to a message before publishing. The rule defines who will see the message, at what time they can see the message and what operations (e.g., like/comment/share) they can do with the message. AID allows users to define rules of how to publish updates on their friends' walls asynchronously. It brings multiple benefits to OSN users. First, it can provide a fair OSN game environment to cope with controversial browser plug-ins (e.g., Snag Bar of Gamers Unite³). AID can also be applied to protect personal privacy if users do not want to disseminate personal news immediately. By employing semantic methods to extract message topics, we will further be able to automatically predict users' preference based on historical events. Besides providing flexibility to OSN users, AID also reduces network traffic and server load by delaying updates, canceling invalid or removed updates and preventing plug-ins from continuously scanning walls. In the near future, we further see a need for more applications leveraging social informatics in order to create and maintain a trustworthy Internet.

³ <http://gamersunite.coolchaser.com/>

References

1. K. Gammon "Networking: four ways to reinvent the Internet" *Nature*, (463)7281, pp. 602-604, 2010.
2. L. A. Cuttillo, et al., "Safebook: a privacy-preserving online social network leveraging on real-life trust," *IEEE Communications Magazine*, vol. 47, pp. 94-101, 2009.
3. D. Boyd, "Social Network Sites: Definition, History, and Scholarship," *Journal of computer-mediated communication*, vol. 13, pp. 210-230, 2007.
4. J. A. Golbeck "Computing and Applying Trust in Web-Based Social Networks", Ph.D. thesis, University of Maryland, 2005.
5. A. Dey "Understanding and Using Context", *Personal and Ubiquitous Computing* 5(1): 4-7, 2007.
6. E. L. Gray "A Trust-Based Management System" Ph.D. thesis, Department of Computer Science and Statistics, Trinity College, Dublin, 2006.
7. M. S. Granovetter "The strength of weak ties" *The American Journal of Sociology*, 1973.
8. D. Boyd "Friendster and publicity articulated social networking" In *Conference on Human Factors and Computing Systems (CHI 2004)*, April 24-29, Vienna, Austria, 2004.
9. L. Garton, et al., "Studying Online Social Networks," Haythornthwaite, et al., Eds., ed: *Journal of Computer-Mediated Communication*, June 1997.
10. C. Skinner, "Phishers target facebook", *PCWorld* (March 01, 2009).
11. R. C. Mayer, J. H. Davis and F. D. Schoorman "An Integrative Model of Organizational Trust" *The Academy of Management Review* (20) 3, pp. 709-734, 1995.
12. J. D. Lewis and A. Weigert "Trust is a Social Reality", *Social Forces* (63) 4, pp. 967-985, 1985.
13. F. Fukuyama "Trust: The social Virtues and the Creation of Prosperity" New York, NY: Simon and Schuster Inc, 1995.
14. M. Spear, X. Lu, S. F. Wu, "Davis Social Links or: How I Learned to Stop Worrying and Love the Net," *IEEE International Conference on Computational Science and Engineering*, pp. 594-601, 2009.
15. B. Cohen "Incentives build robustness in bittorrent," 2003. [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.14.1911>.
16. B. E. Commerce, A. Jang and R. Ismail "The beta reputation system," In the *Proceedings of the 15th Bled Electronic Commerce Conference*, 2002.
17. S. D. Kamvar, M. T. Schlosser and H. Garcia-Molina, "The eigentrust algorithm for reputation management in p2p networks," in *WWW'03: Proceedings of the 12th international conference on World Wide Web*. New York, NY, USA: ACM, pp. 640-651, 2003.
18. L. A. Cuttillo, R. Molva, and T. Strufe "Privacy preserving social networking through decentralization" In *Wireless On Demand Network Systems and Services*, 2009.
19. L. H. Vu, K. Aberer, S. Buchegger and A. Datta "Enabling Secure Secret Sharing in Distributed Online Social Networks," In the *Proceedings of the 2009 Annual Computer Security Applications Conference ACSAC '09*, IEEE Computer Society, pp. 419-428, Washington D.C., 2009.
20. E. A. Baatarjav, R. Dantu, Y. Tang, J. Cangussu, "BBN-based privacy management system for Facebook," In the *Proceedings of the 2009 IEEE International Conference on Intelligence and Security Informatics*, pp. 194-196, 2009.
21. E. A. Baatarjav, R. Dantu, and S. Phithakkitnukoon, "Privacy management for Facebook," In the *Proceedings of the Fourth International Conference on Information Systems Security*, pp. 273-286, 2008.
22. C. Xi and S. Shuo, "A literature review of privacy research on social network sites," In the *Proceedings of the 2009 International Conference on Multimedia Information Networking and Security*, pp. 93-97, 2009.
23. E. Gilbert and K. Karahalios, "Predicting Tie Strength with Social Media," In the *Proceedings of the 27th international conference on Human factors in computing systems*, pp. 211-220, ACM press, 2009.

24. R. L. Punamaki, M. Wallenius, H. Holtto, C.-H. Nygard, and A. Rimpela, The Associations between Information and Communication Technology (ICT) and Peer and Parent Relations in Early Adolescence, *International Journal of Behavioral Development*, 33(6), pp. 556-564, 2009.
25. M. Selfhout, J. Denissen, S. Branje, and W. Meeus "In the Eye of the Beholder: Perceived, Actual, and Peer-Rated Similarity in Personality, Communication, and Friendship Intensity during the Acquaintanceship Process," *Journal of Personality and Social Psychology*, 96(6), pp. 1152-1165, 2009.
26. C. Steinfield, N. B. Ellison, C. Lampe, "Social Capital, Self-esteem, and Use of Online Social Network Sites: A Longitudinal Analysis," *Journal of Applied Developmental Psychology*, 29(6), pp. 434-445, 2008.
27. M. Vaculik and T. Hudecek, "Development of Close Relationships in the Internet Environment," *Ceskoslovenska Psychologie*, 49(2), pp. 157-174, 2005.
28. A. Rybak and F. T. McAndrew, "How Do We Decide whom Our Friends are? Defining Levels of Friendship in Poland and the United States," *Journal of Social Psychology*, 146(2), pp. 147-163, 2006.
29. L. Banks and S. F. Wu, "All friends are not created equal: an interaction intensity based approach to privacy in online social networks," In the Proceedings of the 2009 International Conference on Computational Science and Engineering (CSE), 29-31 Aug. 2009, Piscataway, NJ, USA, 2009, pp. 970-4.
30. M. Katarzyna, "Recommendation system for online social network," ed: Blekinge Institute of Technology, Master's Thesis in Software Engineering, Thesis no: MSE-2006:11, July 2006.
31. T. Tran, J. Rowe, and S. F. Wu, "Social email: A framework and application for more socially-aware communications", *SocInfo '10: Proceedings of the 2nd IEEE International Conference on Social Informatics*, Austria, 2010.
32. T. Tran, et al., "Design and implementation of davis social links OSN Kernel," in 4th International Conference on Wireless Algorithms, Systems, and Applications, WASA 2009, Boston, MA, United states, pp. 527-540, 2009.
33. H. Zhao, S. Ye, P. Bhattacharyya, J. Rowe, K. Gribble, and S. F. Wu, "Socialwiki: Bring order to wiki systems with social context", *SocInfo '10: Proceedings of the 2nd IEEE International Conference on Social Informatics*, 2010.
34. W. Ahmad, A. Riaz, H. Johnson and N. Lavesson "Predicting friendship levels in Online Social Networks", In the Proceeding of the 21st Tyrrhenian Workshop on Digital Communications: Trustworthy Internet, Island of Ponza, Italy, 2010.
35. N. Lavesson, "On the Metric-based Approach to Supervised Concept Learning," PhD thesis, No. 2008:14, Blekinge Institute of Technology, Ronneby, Sweden, 2008. 2010.