Trusty Mechanisms In Social Networks

Antti Relander
Helsinki University of Technology
Antti.Relander@tkk.fi

Abstract

Social Networks have gained major popularity and they are part of everyday life for many people in the world. Social networks are usually based on the idea that you create a network of trust by friending with people you trust. The trusty mechanisms of social networks could have applications in other websites e.g. when you need to evaluate if a person is genuine and trustworthy and not part of a joint fraud. Also trusty mechanisms have applications in social networks them selves. This paper explores the trusty mechanisms in social networks and their applications outside and inside the network. We evaluate the current possibilities and shortcomings of social networks. Finally we propose what possibilities there is to make the trusty mechanisms more accurate and how to overcome the problem of joint fraud associated to social networks.

KEYWORDS: Social networks, trust, recommendation systems

1 Introduction

Social networks are part of everyday life for many people. According to statistics of Facebook the service has now over 350 million users and the average user spends 55 minutes on the page and has 130 friends on her network. [1]

Facebook is taken into special concern in this paper because it's the largest social network service at the moment. Popularity has grown so far that even some dictionaries like The Oxford Dictionary have added words like friending and unfriend to their dictionaries.

Traditionally trust in the online world is based on a reputation of entities. You trust a website that is well known e.g. a popular reliable news source like The New York Times website or a government website. This trust is increased by using encryption based on trusted 3rd party certificate authorities that verifies that the source really is the one that it's claimed to be. However, this approach is not always applicable when we are dealing with ordinary people who don't have a well-known reputation.

The trusty mechanisms in social networks vary but the concept is almost always the following: When you join a social network you start to make connections with the people you like to share information with and form your own network of trust.

The privacy settings vary between the social network sites but there has been a debate in media about the privacy settings that might allow people outside your social network to access your private information.[2] [3]. Sometimes this is relevant when someone in your social network does something with you and a friend of that person - a multi-hop user - gets this information of this action. However, this can lead to unwanted situations and the user has to know how to cope with privacy settings. Latest example of privacy issues on the news was an issue with newcomer google buzz where the default settings automatically shared your writings globally to everyone. [2]

All theses mentioned examples results from trusts issues. You want to share personal information to your network but you don't necessary want to share it to anybody else. [4] With better trusty mechanisms this issue could be fixed. However, it should be noted that trust in online context is no different from the trust in the real world in the context that even your closest friends can always betray you. Trust typically takes a long time to build up but it can collapse fast [5]. (There are some (funny) websites that exploits the trust in the social networks (anonymously though) such as www.failbooking.com.)

Trust in the online world can be measured with various trust metrics used for different purposes. [6] One example of a trust metric is Ebay's Feedback Rating. The metric rates sellers according to the feedback from previous sells and it also has been proposed to use a social network data as trust metric in social network research. [7]

A key finding would be to find a universally working and unexploitable trust metric and mechanism that could be used with existing social networks and applications outside the network. We will look into this in the last chapters. The problems are that there's always a party that will benefit from exploiting the system in terms of real money or for example a social status. Such an example would be a joint-fraud where group of people or bots will increase a trustworthiness of an entity that wouldn't otherwise deserve it. [7]

The paper structure is the following. First we take a look at the current situation of social networks and their opportunities and challenges. Then we discuss how the users' identity could be expressed and how the trust relationships between users can be expressed formally. Finally we propose a solutions to multi-hop user trust issue and the problem of joint fraud.

2 Requirements

Trust itself is mental state of a person that cannot be directly measured but it has a mathematical foundation.[5] [8] This mathematical foundation can be used when applications for trust are researched. A certain trust metric can be used to

measure a trust in a social network. That metric can be used to evaluate a trust of peer for business purposes. [6]

3 Opportunities

Opportunities of social networks vary from business opportunities to subjective value of sharing and obtaining information that is the basic functionality of a social network. The essential part of the opportunities derives from the fact that social networks accomplish trust between entities. Social networks form trust networks between peers. This network of trust can be then translated to business opportunities. For these values to become real, a network needs to form a critical mass of the peers.

3.1 Existing social networks

There are various different social networks and new ones are coming now and then. At the moment the top five in terms of registered users according to listing in Wikipedia is following: Facebook, Qzone, Orkut, MySpace, Windows Live Spaces [9]. It's interesting to notice that second biggest social network is Chinese. Overall the growth of the networks has really been exponential. The largest social network - Facebook - was founded in 2004 and opened to the public (for all the people over 13 years of age) in 2006. [10]

The size of the network matters and the Metcalfe's law - or more effectively the derived Reed's law can be applied to social networks. [11] [12], The value of the network is proportional to the square of the number of nodes.[13] In social networks according to the Reed's law the proportion is closer to 2^n because a social network can be divided to sub networks [12]. This has importance for both the subjective value and business value.

3.2 Functions on social networks

The basic function of social network for users is to connect with his/her friends and possibly connect with new friends also. Social networks provide a great platform for sharing information, private moments, thoughts, photos and videos for the users. [14] Users regard social networks as valuable and reliable sources of information about a person. [15] A persons trustworthiness can be evaluated using the data gathered from a social networking website. [15] This trustworthiness still is subjective because tend to have different opinions of trustworthiness of a person. [8]

Trust mechanisms can be used in existing social networks when friends are being suggested to users. [16] To add value to the user social networking sites can recommend people to make friends with people who they evaluate as trustworthy to that person. This brings value if a system can connect two people with same interests that don't know each other. [16]

3.3 Business opportunities

Social networks are usually proprietary systems that might have a open API for software developers to build softwares that uses the data from the social network. This approach gives opportunities for skilled people to create business by developing software over the social networks. This type of software is useful to the owner of the social network because it enhances the lock-in effect and the value of the website.

Social network users share their personal information that the social networks sites them selves can use to create targeted advertisements. Targeted advertisements can be generated some might say dangerously precisely according to the personal details of the user. People use plenty of time to view social networking websites and targeted advertisements can be more attractive than traditional banner advertisements.

Trust mechanisms of social networks could be applied in situations where a trustworthiness of a person needs to be evaluated. We can consider a situation where a new employee is applying a job. It's likely that the employer will evaluate the candidates social network profile to verify the trustworthiness of that person. For example a popular social networking site LinkedIn (www.linkedin.com) is based on the idea of making new business contacts based on the trust of the existing ones.

Marketing products or services are also possible in the social networks. Viral marketing strategies that use network effects are much cheaper than the usual advertisement based marketing strategies. For example if a new product comes to the market and needs to be promoted it's effective marketing strategy to get people in the trust networks to promote the product for manufacturing company. Research shows that user's get more satisfaction from the transactions in their own social networks but further research is needed to evaluate the effects of viral marketing [17]

One proposal is to use social network as an authentication tool [18] or a indication of reputation. [7] [19] [20] [21] The trust mechanisms of social networks provides a reliable indication of trust that can be used for building reputation. [7] [19] [20] [21] Problems with reputation tools arises from new users joining the community [22] and the problem with malicious users. [7] [19] [20]

As an authentication tool the idea is that a data such as photos gathered from user's social network can be used when it's needed to distinguish a genuine user from a bot. The concept here is to replace commonly used CAPTCHAs with an authentication method that uses photos where user is tagged from user's social network and question the other people in that photo. [18]

4 Challenges

Some of the opportunities require information from users that can be seen as private information such the structure of personal social network. Some users are not willing to share their personal information. This is due to the fact that users are becoming aware of the risks if they share sensitive data publicly. [4] If anonymity is needed for service, social network data cannot be used either. Anonymity and fair user discrimination is violated, if users are required to have a social network account in major services like Facebook. Social network id cannot be therefore be a required identification like IP address.

Because people are in control on social networks - as they are networks of people - one can only predict a behavior of

individual people or a group. Formed trust can be unexpectedly collapse and it's virtual impossible to predict it. A malicious user can pretend to be and act as a legitimate user for long time before betraying the trust similarly to real life con scenarios.

4.1 Shortcomings on social networks

Privacy is one they key issues when talking about social networks. Users usually share private information that malicious person can use for identity theft among other possible crimes with sensitive personal data. [3] [23] Social networks are also gateways to spread private data, if members of the users social network or a multi-hop user spreads them. [23] This might lead to situations where for example embarrassing pictures spreads outside the network of trust. It has been proposed that social trust could be used as an access control tool instead of user controlled access tool. [24]

Taken that almost all social network sites use different proprietary systems to build networks there is no standard how to design and build a social network site. This means also that it is at the moment impossible to interconnect a social network to another and users needs to be part of every social network site he/she wants to be a part of. This leads to a strong lock-in effect. When user is part of one social network and wants to switch to another it is virtually impossible to have the same value if all the members of his/her social network don't do the same.

The software widgets build upon the social networks have become a successful business as mentioned in chapter 3.3. However, this also has a darker side. Some of the applications can be considered as spam according to the users and some of them try to gather private information from the users and use it for disrespectful purposes. [23]

4.2 The trusty problems in the social network

Trust problems occur due to various reasons. Firstly users are not aware or don't care about the access control and privacy settings that might sometimes lead to unwanted situations.

Secondly, it's not too uncommon that people in the social networks friend with people who they have not ever met or don't really know at all. If you trust a person you don't know it can compromise and your personal information and give a false indication of trust for others.

Thirdly, sensitive private information could be compromised if an account is unauthorizedly accessed. It not only compromise that user's data but all of the friends are compromised as well. Access to account will also give an intruder the possibility to effect the trust relationships of the breached account.

4.3 The problem of joint fraud

A joint fraud in this context is a type of collusion where a group of people act cooperatively towards a common goal to deceive other users. Malicious users can form a group to gain trust that can be used to cheat a trust metric or actual individuals. [23] Application of a joint fraud is for example boosting up a reputation rank in an online store. Joint fraud is important in this context because it's a result of system that relies on the trust mechanisms of social networks. A cleaver algorithm is needed to detect a joint fraud.

5 Policy on trusty mechanism of social network

Efficient policy for a trust mechanism needs to bring value to users by taking account the privacy of the users without compromising the usability too much. It also needs to take account trust exploiting possibilities of current solutions. [25]

5.1 The general expression mode of users' identity

The most obvious solution here would be to demand a certification from the users of the social network to verify who they really are. This would solve the problems related to false identities and bogus persons. If all the users would be verified people could really trust that they are who they claim to be. At the moment the identities of the users is verified through email verification. Issue with email verification is that it's trivial for a person to create bogus and false identities and it only merely blocks computer generated identities. A new system that uses a stronger verification such as an E-bank account or national electronic identity could be generated to handle the verification process instead.

This approach still has major concerns and fallbacks. This would at first result in major costs. Implementation of such a system is not trivial because there is no universal way to verify a person reliably electronically. It's likely that all users could not be verified especially those who live in developing countries where electronic verification methods rarely exists. The most global form of verification would be verification by a credit card but this would again limit the user space to credit card holders only. The major problem with this type of verification is also that it will result in difficulties in case of identity theft. However, on the business perspective it would open up opportunities if the people could use their social network accounts for transactions. I see that this type of approach could happen in the near future when electronic verification develops enough.

Easier approach here could be the use of existing social network and instead of trusted 3rd party and let the members of the network decide who is trustworthy. [7] Members of an user's social network could verify that the user is who user claims to be. Users are likely to distinguish false identities and bogus users from the real ones. This could be done by polling all the users to verify their members to verify their friends or one might say that this is not even necessary because the bogus users don't likely have a large social network. This type of identification method is easy to implement but it hides an internal problem of joint fraud in it. A group of people could verify a false identity to be a real one. At the moment identification usually works kind of other way around where user's can report malicious users to the maintenance. One might say that the identification of social networks are strong enough already.

It should be noted that none of the identification methods would resolve trust related problems such as joint-fraud where legitimate people maliciously co-operate. In addition to identification there should be a reliability metric to measure a reputation of an identity to avoid these type of issues.

5.2 The expression mode of trusty mechanism between users

Trust in social networks can be expressed by a trust metric. A trust metric can determine how trustworthy another person is to the user, but because of the nature of trust is subjective, a common algorithm for a trust mechanism is hard to derive. [15] User should have a control of the trust on social network like in the real life. [3] [25]

A trust metric in social network context can be based on the links between users. The previous works in this field have been concentrated on reputation of websites and P2P systems. [26] There are solutions like Eigentrust that evaluates trust between nodes in P2P networks [27] [28] and peer-trust [26]. As P2P networks are somewhat similar to social networks - as they are connections between real people - these type of metrics might be relevant in social networks also. Probably the most well-known trust metric in the world is Google's patented PageRank that evaluates the trustworthiness of website links. An algorithm similar to PageRank called NodeRank can be used when evaluating links in social networks. [7] This approach has been criticized because connection based trust assessment hides the fact in human psychology trust is multi-dimensional and result of various parameters rather than connections. [15] [16] Trust evaluation should take account other activity related information such as profile information, comments and internet activity of the user because that's they way the users evaluate trust in psychological context. [15]

Another approach is to evaluate the trust in social networks by parametrizing the connections in social networks by the activities on the network [28]. This is done by evaluating trust by how often the peers in the network communicate with each other and the more they do the more they trust each other [28]. A combining method has been researched that composes of trust relationships, influential and environmental factors. [29] This model exists only in theory but it still is the most promising one.

It's possible to evaluate trust by comparing profile similarities in social networks. [30] But this merely indicates the real psychological trust between users if they only have same interests.

Completely different approach is to redesign the social network architecture and instead of web-based centralized applications use a distributed P2P network to implement a social network and increase it's trustworthiness. [19] [28] But this approach would need further research to increase performance and usability. [28] Interaction based trustworthiness assessment can have applications in e-commerce communities where a reliable review and recommendation systems provide value to customers. [19]

5.3 The expression mode of trusty mechanism of multi-hop users

Users should have control of privacy in social networks. Users should be able to decide whether and what information multi-hop users can see. In many cases it makes sense to share some information to peers that the peer don't know or trust but in many cases there are some information that peers only want to share within their own trust networks. [3] [4] In Facebook for example a user can very specifically determine what information is shared and who can access it. It's hard to determine whether a multi-hop user is trustworthy or not when that user is not in the user's social network.

A trivial solution for a metric here would be to count the mutual friends between the user and a multi-hop user and determine the trust that way. Such an algorithm exists an it's called TidalTrust. [31] This could be possibly be applicable in economical sense but in sociological sense and using the common sense this is not however a good solution because in large communities there is usually people who have mutual friends but haven't never met and therefore a trust enabling social connection hasn't formed. People don't always cope well with other people and case can also be that even though two peers have many mutual friends they actually distrust each other or have had trust conflicts in the past. This derives from the fact that trust is usually unidirectional and subjective. [8]

5.4 How to solve the problem of joint fraud

A solution to the joint fraud problem can relay inside the social networks. If a strong identification is used - people use their real identities - and social network data is used a collusion detection mechanism can be built. This idea is based on a fact that when measuring reputation by excluding the nearest connections to friends. [7]

Another strong candidate for a solution of the joint fraud problem and in general a social network with malicious users is SocialTrust framework. [23] This framework bases it's ideas to the connections and the qualities of these connection on social networks [23]. SocialTrust is according to the research [23] more efficient in precision compared to the PageRank and TrustRank trust assesment algorithms.

References

[1] Wikipedia, "Facebook official website," 2010. [Online; accessed 17-March-2010].

[2] B. Maggie Shiels, "Google buzz 'breaks privacy laws' says watchdog," 2010. [Online; accessed 17-March-2010].

[3] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and privacy concern within social networking sites: A comparison of facebook and myspace," in *Proceedings of the Thirteenth Americas Conference on Information Systems (AMCIS)*, 2007.

[4] O. Nov and S. Wattal, "Social computing privacy concerns: antecedents and effects," in *CHI '09: Proceed-*

ings of the 27th international conference on Human factors in computing systems, (New York, NY, USA), pp. 333–336, ACM, 2009.

[5] Wikipedia, "Trust — Wikipedia, the free encyclopedia," 2010. [Online; accessed 17-March-2010].

[6] Wikipedia, "Trust metric — Wikipedia, the free encyclopedia," 2010. [Online; accessed 17-March-2010].

[7] T. Hogg and L. Adamic, "Enhancing reputation mechanisms via online social networks," in *EC '04: Proceedings of the 5th ACM conference on Electronic commerce*, (New York, NY, USA), pp. 236–237, ACM, 2004.

[8] J. Golbeck and J. Hendler, "Inferring binary trust relationships in web-based social networks," *ACM Trans. Internet Technol.*, vol. 6, no. 4, pp. 497–529, 2006.

[9] Wikipedia, "List of social networking websites — Wikipedia, the free encyclopedia," 2010. [Online; accessed 17-March-2010].

[10] Wikipedia, "Facebook — Wikipedia, the free encyclopedia," 2010. [Online; accessed 17-March-2010].

[11] J. Hendler and J. Golbeck, "Metcalfe's law, web 2.0, and the semantic web," *Web Semant.*, vol. 6, no. 1, pp. 14–20, 2008.

[12] Wikipedia, "Reed's law — Wikipedia, the free encyclopedia," 2010. [Online; accessed 17-March-2010].

[13] Wikipedia, "Metcalfe's law — Wikipedia, the free encyclopedia," 2010. [Online; accessed 17-March-2010].

[14] Wikipedia, "Social network — Wikipedia, the free encyclopedia," 2010. [Online; accessed 17-March-2010].

[15] S. ten Kate, "Trustworthiness within social networking sites: A study on the intersection of hci and sociology," *Master Thesis*, 2009.

[16] P. De Meo, A. Nocera, G. Quattrone, D. Rosaci, and D. Ursino, "Finding reliable users and social networks in a social internetworking system," in *IDEAS '09: Proceedings of the 2009 International Database Engineering & Applications Symposium*, (New York, NY, USA), pp. 173–181, ACM, 2009.

[17] G. Swamynathan, C. Wilson, B. Boe, K. Almeroth, and B. Y. Zhao, "Do social networks improve e-commerce?: a study on social marketplaces," in *WOSP '08: Proceedings of the first workshop on Online social networks*, (New York, NY, USA), pp. 1–6, ACM, 2008.

[18] S. Yardi, N. Feamster, and A. Bruckman, "Photo-based authentication using social networks," in *WOSP '08: Proceedings of the first workshop on Online social networks*, (New York, NY, USA), pp. 55–60, ACM, 2008.

[19] H. Liu, E.-P. Lim, H. W. Lauw, M.-T. Le, A. Sun, J. Srivastava, and Y. A. Kim, "Predicting trusts among users of online communities: an epinions case study," in *EC '08: Proceedings of the 9th ACM conference on Electronic commerce*, (New York, NY, USA), pp. 310–319, ACM, 2008.

[20] Y. Matsuo and H. Yamamoto, "Community gravity: measuring bidirectional effects by trust and rating on online social networks," in *WWW '09: Proceedings of the 18th international conference on World wide web*, (New York, NY, USA), pp. 751–760, ACM, 2009.

[21] P. Massa and P. Avesani, "Trust-aware recommender systems," in *RecSys '07: Proceedings of the 2007 ACM conference on Recommender systems*, (New York, NY, USA), pp. 17–24, ACM, 2007.

[22] P. Victor, C. Cornelis, A. M. Teredesai, and M. De Cock, "Whom should i trust?: the impact of key figures on cold start recommendations," in *SAC '08: Proceedings of the 2008 ACM symposium on Applied computing*, (New York, NY, USA), pp. 2014–2018, ACM, 2008.

[23] J. Caverlee, L. Liu, and S. Webb, "Socialtrust: tamper-resilient trust establishment in online communities," in *JCDL '08: Proceedings of the 8th ACM/IEEE-CS joint conference on Digital libraries*, (New York, NY, USA), pp. 104–114, ACM, 2008.

[24] B. Ali, W. Villegas, and M. Maheswaran, "A trust based approach for protecting user data in social networks," in *CASCON '07: Proceedings of the 2007 conference of the center for advanced studies on Collaborative research*, (New York, NY, USA), pp. 288–293, ACM, 2007.

[25] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin, "Persona: an online social network with user-defined privacy," in *SIGCOMM*, pp. 135–146, 2009.

[26] L. Xiong and L. Liu, "Peertrust: supporting reputation-based trust for peer-to-peer electronic communities," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 16, no. 7, pp. 843–857, 2004.

[27] 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), pp. 640–651, ACM, 2003.

[28] O. Schneider, "Trust aware social networking: A distributed storage system based on social trust and geographical proximity," *Master Thesis*, 2009.

[29] X. Zhang and Q. Zhang, "Online trust forming mechanism: approaches and an integrated model," in *ICEC '05: Proceedings of the 7th international conference on Electronic commerce*, (New York, NY, USA), pp. 201–209, ACM, 2005.

[30] J. Golbeck, "Trust and nuanced profile similarity in online social networks," *ACM Trans. Web*, vol. 3, no. 4, pp. 1–33, 2009.

[31] Y. Katz and J. Golbeck, "Social network-based trust in prioritized default logic," in *AAAI'06: proceedings of the 21st national conference on Artificial intelligence*, pp. 1345–1350, AAAI Press, 2006.