SJIF 2013 = 1.795
ISSN: 2348-3083
An International Peer Reviewed & Referred
SCHOLARLY RESEARCH JOURNAL FOR
HUMANITY SCIENCE & ENGLISH LANGUAGE

SECURITY AND PRIVACY ISSUES ON SOCIAL NETWORKING SITES: AN ANALYSIS ON ATTACKING SCENARIOS

Mr. Kishor Keshaorao Wikhe & Arjun Pralhad Ghatule, Ph. D.

Abstract

Protecting personal information's privacy has become a controversial issue & liability among online social network providers and users. Most social network providers have developed several techniques to decrease threats and risks to the users' privacy. These risks include the misuse of personal information which may lead to illegal acts such as identity theft, predators, stalking, online victimization, and fraud. To give few examples, in May 2015 Russian hackersemployed malware to target a number of banks worldwide stealing upwards of $900 million in one year alone. Russian hackers also developed iOS7 malware designed to access user's personal data. This study aims to measure the awareness of users on protecting their personal information privacy, as well as the suitability of the privacy systems which they use to controlprivacy settings. Survey results show high penetration and high percentage of the use of smart phones for dataservices but the current privacy settings for online social networks need to be improved to support different type of mobile phones. Because most users use their mobile phones for Internet services, specific privacy settings that are compatible with mobile phones need to be developed. The method of selecting privacy settings should also be simplified to provide users with a clear picture of the data that will be shared with others. Results of this study can be used to develop a new privacy system which will help users control their personal information easily from different devices, including mobile Internet devices and computers.

Keywords: *Privacy, Security, Theft, Fraud*

1. INTRODUCTION

Misrepresentation is a wrongdoing where the intention is to usurpcash by an unlawful means. Misrepresentation bringsexpansive and expensive misfortunes to organizations or States or individuals. Since its identification is unpredictable and ever improvising, there is not yet a misrepresentation structure or algorithm that can distinguish and avoid extortion in an effective way. Any business or personal undertakings that include cash and administration can be traded off by false acts. Such domainsas Social Security, Insurance, Telecommunications, Financial and Credit Cards are cases of where extortion may happen and where, in the current past, there has been a push to create techniques to battle this sort of unwarrantedmisrepresentation. Every one of the problems has peculiar attributes; in this manner, a solitary arrangement that might be sent to battle extortion in Credit Cards can't be connected to Insurance industry. As a result, one of the ways to deal with battle extortion is to seek after a model that depicts false practices, or, better, make components that recognize deceitful from non-fake practices. In fact, these instruments can be made utilizing an information mining arrangement, making utilization of an arrangement of verifiable records, i.e., records of past customers definitely known as false and non-fake (the preparation set or training set). Notwithstanding, applying grouping procedures for battling misrepresentation dependably manages a disposition: the presence of a lopsided preparing (training) dataset – a set that has numerous non-fake records and just a couple of deceitful cases which may not be true representative datasets. Due to this peculiar situation, the consequence of applying customary algorithmprocedures, similar to choice (or decision) trees orself-learning neural systems, are insufficient and inadequate for getting a decent classifier with reasonable accuracy and precision. With regards to grouping, there are three noteworthy methodologies that may be used to make a classifier for misrepresentation identification: adjust the information, consider diverse mistakes costs and identify exceptions. This paper portrays &characterizes misrepresentation and what are the issues related with arrangement calculations, when one endeavors to recognize and foresee extortion. Alongside this portrayal, it shows an arrangement of most utilized systems to confront the expressed issues. Finally, it remarks on the particularities of some business regions that are influenced by misrepresentation. The particular issue that will be tended to be this paper is extortion location at the ―DirectorGeral de Impostos‖ (that is in a free interpretation to the State Taxes Organization) on the Value Added Tax (VAT), specifically on the recognition concerning Carrousel misrepresentation cases. Along these lines, one of the destinations of this paper is to build up a misrepresentation classifier, with a worthy exactness level for false cases. In addition, this must be proficient by fathoming or limiting budgetary misrepresentation identification issues. Keeping in mind the end goal to get this objective, a few classifiers will be made, executing the most important methodologies for misrepresentation location, as systems to adjust the dataset or calculations that learn with various blunders costs. Alongside this, recall extortion is sustained by individuals or by associations that can't segregate themselves from whatever is left of the world. Thus, fake people and associations are associated among themselves and to whatever remains of all other genuine and reasonable associations. It is, truth be told, is critical not to manage substances independently, when searching for misrepresentation at the same time, likewise, to manage the connections between these elements. For instance, the proprietor of a false association is most likely the individual in charge of the extortion itself. On the off chance that he claims another association, it is more probable that this second association is likewise fake. Another issue is the way that some exploit carrousel extortion, which must be refined with a connection of a few associations. Along these lines, the investigation of interpersonal organizations inside deceitful associations and its kin&office bearers can be critical when hunting down misrepresentation. In this way, with the work exhibited here, the interpersonal organizations in every association will be broken down keeping in mind the end goal to identify designs that are normal to fake associations. These examples will uphold the information in VAT revelations, keeping in mind the end goal to make a dataset with more valuable data. The dataset is the base support for the formation of new classifiers, which will be a great deal more precise than the first ones. With this new dataset that, in spite of the fact that having more data about every association is still an uneven dataset, to which it will be additionally connected certain systems do manage that particular issue. (Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke (2007))

Extortion is characterized by the Association of Certified Fraud Examiners as ―the utilization of one's occupation for individual enhancement through the consider abuse or use of the utilizing association's assets or assets‖ and by the Cambridge Advanced Learner's Dictionary as ―the wrongdoing of acquiring cash by misdirecting people‖. These definitions show that extortion is, actually, a wrongdoing in which the its goal is to get cash in an illicit frame, just by exploiting a position or power in a business association and utilize them for unseemly expectations alongside the assets and devices of the association. This in appointment of products and ventures can be refined by a solitary individual, with the goal of individual increases or by and large by an association itself. It is a given that misrepresentation is a wrongdoing as old as time. These days, with the development of innovation, upheld by worldwide and expedient correspondence system, is less demanding and quicker to sustain extortion, being substantially more muddled to be identified. False exercises prompt to largess monetary misfortunes worldwide for both business and States. Therefore, it is critical at the present in time of financial emergencies to recognize and battle extortion, with a specific end goal to perhaps recoup cash taken. Alongside this, with the development of innovation, new sorts of misrepresentation have emerged, for example, media transmission extortion, PC interruption, social security number theft, charge cards and protection extortion. Every business territory conveys its own particular extraordinary elements thus the strategies for distinguishing and battling misrepresentation must be distinctive, when managing every sort of business. To muddle matters considerably more, colossal measures of information is created each year and, along these lines, more productive systems to dig that information looking for fake data is important (Kou, 2004) (Hilas, 2005).

One approach to break down and battle extortion is by applying Data Mining, which is the exploratory period of picking up information in databases handle (KDD). This errand is characterized as ―the non-paltry extraction of verifiable, past obscure and conceivably valuable data from data‖ (Adriaans, 1996). Information mining employeesand arrangement of procedures that assistance to reach at key data that may prompt to extortion information,one of these strategies is the development of a grouping model, which endeavors to distinguish characteristic examples of extortion in various zones of business (Weatherford, 2002).

2. REVIEW OF LITERATURE

The information used to empower misrepresentation recognition has particular qualities that cause three fundamental issues worth tending to, which must be managed when working with the information. Qiong Wei, Yansheng Lu (2008)the primary fundamental issue is brought on by the unequal conveyance of the information, where one needs to manage datasets that have not very many false records, contrasted and the non-fraudulent ones. In these datasets, where a class has most of the cases, standard classifiers have a tendency to disregard the minority information class (VO, 2007). The second issue is the diverse blunders and expenses of the misclassification of the information itself. The cost of misclassifying a deceitful record as non-fake is much higher than misclassifying a non-fake as fake (Hall, 2001). The third issue, yet not small, is the discovery of records that go amiss from the typical dissemination of the dataset. These records are known as exceptions and can, truth be told, be markers of potential fake exercises. There are two diverse ways to deal with managing the uneven dataset issue. The first, typically done in the pre-preparing stage, comprises in the reconfiguration of dataset into a more adjusted one. This should be possible by disposing of a portion of the occasions in the lion's share class or by producing more occurrences of the minority class. The second approach in managing the uneven dataset is the utilization of boosting calculations. Boosting calculations are iterative calculations that utilization diverse weights on the preparation set dispersion on every cycle. Modifying the weights or by expanding the case of the misclassified and diminishing the event of the right ordered examples, the calculation will concentrate more on the misclassified occasions, which are all the more regularly deceitful occurrences. Since the mistake cost of misclassifying a false examples is higher than the blunder cost of misclassifying a non-fake events, it is critical to concentrate not just the accuracy (rate of right characterized cases) in any case, additionally, to the sensibility (rate of right grouped deceitful occasions) of every case. Other than these more specialized issues, there is an applied issue that is not mulled over when building classifiers utilizing a dataset that is framed only by information taken from tax documents or public domain. This issue is upheld by the way that an association is not one of a kind and remains solitary on the planet. Associations are based on connections between different associations and individuals themselves. Remembering this, it is critical to take a gander at the informal community of every association. Because of this dynamic condition, the identification of informal community designs, in the false associations, can help the development of a superior information classifier. Hence, apparatuses are expected to assess if every association has an example of social connections like the deceitful ones and, subsequently, utilizes the data to help with the order stage. Taking everything into account, the utilization of strategies to adjust the dataset and the utilization of informal community examples to improve the dataset are two of the procedures that, when consolidated, create better outcomes in the ID of false associations.

Kaufman et al. (2008) introduce a new social network dataset site Facebook.com with findings to exemplify the scientific and pedagogical potential of this new network resource with a future prospect in this area of research. Since social network research embodies a range of expertise from Anthropology to Computer Sciences, it is quite difficult to find the benchmarks for social networks. Further, social networks have been measured on various datasets including online social reach to special interest networks. The authors propose a method by using formal concept analysis in understanding the social networks with ease in analysis and visualizing the networks and propose to use bigger networks in future. Social data mining is used to improve bioinspired intelligent systems with swarm optimization, ant colony and cultural algorithms.

Abraham et al. (2009) addressed the computational complexity of social networks analysis and clarity of their visualization that uses combination of Formal Concept Analysis and well-known matrix factorization methods. The goal is to reduce the dimension of social network data and to measure the amount of information which is lost during the reduction. Singular value decomposition has already been used in the field of social network data to determine the position of nodes in the network graph.

Abraham et al. (2009) try to consider a Web page as information with social aspects. Each Web page is the result of invisible social interaction. For the description of the social aspects of Web pages, they used the term Micro Genre with fundamental concepts of Micro Genre with an illustration to the experiments for the detection and usage of Micro Genres.

Zhou et al. (2009) build up a social network mining solution to discover the social network, users' relationship, key figures and impaction to the organization on BBS website in order to understand the internal and external association of an organization so as to enhance the collaboration and disseminating knowledge.

Markus Huber, Martin Mulazzani, and Edgar R. Weippl. (2010). within this research, they present novel friend injection attack which exploits the fact that the great majority of social networking sites fail to protect the communication between its users and their services. The friend injection attack enables a stealth infiltration of social networks and thus outlines the devastating consequences of active eavesdropping attacks against social networking.

3. SECURITY AND PRIVACY ISSUES

Social networking sites have become very popular avenues for people to communicate with family, friends and colleagues from around the corner or across the globe. While there can be benefits from the collaborative, distributed approaches promoted by responsible use of social networking sites, there are information security and privacy concerns. The volume and accessibility of personal information available on social networking sites have attracted malicious people who seek to exploit this information. The same technologies that invite user participation also make the sites easier to infect with malware that can shut down an organization's networks or devices, or keystroke loggers that can steal credentials. Common social networking risks such as spear phishing, social engineering, spoofing, and web application attacks attempt to steal a person's identity. Such attacks are often successful due to the assumption of being in a trusting environment social networks create.

Security and privacy related to social networking sites are fundamentally behavioral issues, not technology issues. The more information a person posts, the more information becomes available for a potential compromise by those with malicious intentions. People who provide private, sensitive or confidential information about themselves or other people, whether wittingly or unwittingly, pose a higher risk to themselves and others. Information such as a person's social security number, street address, phone number, financial information, or confidential business information should not be published online. Similarly, posting photos, videos or audio files could lead to an organization's breach of confidentiality or an individual's breach of privacy by social engineering. When it comes to privacy and security issues on social networks, the sites most likely to suffer from issues are the most popular ones example face book and twitter. Security issues and privacy issues are entirely two different beasts. A security issue occurs when a hacker gains unauthorized access to a site's protected coding or written language. FANG (2010) Privacy issues, those involving the unwarranted access of private information, don't necessarily have to involve security breaches. Someone can gain access to confidential information by simply watching you type your password. But both types of breaches are often intertwined on social networks, especially since anyone who breaches a site's security network opens the door to easy access to private information belonging to any user. But the potential harm to an individual user really boils down to how much a user engages in a social networking site, as well as the amount of information they're willing to share. LIPFORD (2008)

The reason social network security and privacy lapses exist results simply from the astronomical amounts of information the sites process each and every day that end up making it that much easier to exploit a single flaw in the system. There is an exposure in potentially devastating hole in the framework of Facebook's third-party application programming interface (API) which allows for easy theft of private information. It has been found that third-party platform applications for Facebook gave developers access to far more information (addresses, pictures, interests, etc.) than needed to run the app. This potential privacy breach is actually built into the systematic framework of Facebook, and unfortunately the flaw renders the system almost indefensible. There are many issues like

a. The question for social networks is resolving the difference between mistakes in implementation and what the design of the application platform is intended to allow

b. There's also the question of whom we should hold responsible for the over-sharing of user data?

That resolution isn't likely to come anytime soon, because a new, more regulated API would require Facebook - to break a lot of applications, and a lot of companies are trying to make money off applications now. It is also true that “now there are marketing businesses built on top of the idea that third parties can get access to data on Facebook." Since social networks are all about “friends,” getting hold of a victim's account will provide the hacker knowledge of that victim's circle of friends. Once the hacker has access, they can pose as a trusted friend, creating phishing messages containing links to malware or including malware-laden files. Because the messages purportedly come from a “friend,” the victim may be more susceptible to follow the links or open the attachments. A method has been established to gain access to the account of a specific user is getting the password. But how can this are accomplished? There are myriad ways:

- Malware: Keystroke loggers can record a user's activity, including passwords for different applications. This malware can be installed through social engineering techniques circulated via email or over a social network, like Facebook, that encourage a user to download a malicious application masquerading as a legitimate one.

- Phishing: By creating a mock login page, hackers can attempt to deceive users into divulging their login credentials. Once the hackers have the login information, they can then access the user's profile, gaining access to their network of friends and other personal information.
- Bruteforce: Hackers can repeatedly attempt to guess a user's password. This technique can be especially effectiveagainst users with easy-to-guess passwords, like "password" or "12345."
- Social Engineering: Use of deception and covert seemingly friendly techniques to manipulate unsuspecting people in divulging personal or organizational information that can be used for fraudulent purposes.

Hackers communicate with each other in online hacking forums, selling services to teach other hackers how to use the above methods to breach the accounts of unsuspecting users. If users don't take the appropriate precautions to protect their social networking profiles, there can be nasty consequences – not just for the user, but also for their employers, families and greater communities.

The MilitarySingles.com, a dating website for members of the military, was compromised by hackers, resulting in the publishing of names, email addresses and passwords for more than 150,000 of the site's members. This breach was likely caused by uploading a malicious file masquerading as a .JPEG attachment on the website.

The pervasiveness of web applications, combined with the tendency of social media users to increasingly reveal private information, can create a serious security risk. In the case of MilitarySingles.com, the personally identifiable information of members of the U.S. military was accessed, giving hackers access to the email accounts of military members and, arguably, access to potentially damaging secrets.

4. ATTACKING SCENARIOS

Privacy related threats -

a) Digital dossier aggregation: SNS profiles can be fetched and stored by third parties in order to create a digital dossier of personal data. Hogben et al. argue that due to diminished costs of disk storage and Internet downloads it is feasible to take incremental snapshots of entire SNSs. A proof-of concept digital dossier aggregation, carried out on an early version of the most popular German SNS (meinVZ), showed that 10,74,574 profiles could be aggregated within less than four hours with a computer cluster consisting of ten computers. Highlighted various methods how data could be collected from Facebook. Furthermore showed that information that is publicly available could be used to infer the social graph of SNSs users,a commercial provider even offers packages for crawling social networks which can be used to aggregate publicly available information.

b) Secondary data collection vulnerabilities: SNS members also disclose information to their Internet service providers (ISPs). While this is not solely limited to SNSs, the main difference is the extent of coherent personal data exposed to ISPs. For example to map the circle of friends without SNSs data, ISPs need to correlate information from multiple Email addresses, instant messaging, etc. Even more important is the threat of disclosure and resale of personal information to third parties, for example to providers of targeted advertisement. At the time of writing no case of secondary data collection has been documented. A recent case with AT&T however illustrated how serious this threat is.

c) Face recognition vulnerabilities: SNS users provide profile images of themselves and SNSs contain shared images associated with them. Face recognition technology can be used to identify users across different SNSs, no matter if pseudonyms or fake names are being used.

d) CBIR (Content-based Image Retrieval):CBIR is a technology which deduces the location of users by analyzing and comparing common patterns in images. Hence shared images within SNSs not only disclose the identity of users but possibly the location of users as well.

e) Click jacking: This is another type of attack scenario in which attacker posts some videos or post to the victim and when victim clicks on the page some malicious actions are performed. This is common in Facebook with the name like jacking that is when a user likes a page, a picture or a video the user is trapped by the attackers. This type of attacks are done to do malicious attack or to make some page popular.

f) Neighborhood Attack: The neighborhood attacks are done by the attackers by knowing the victim's neighborhood. It means the attacker knows the friends of the victim. Attacker uses the relationship among these friends and based on this relationship tries to identify the victim.

g) Linkability from Image Metadata, Tagging and Cross profile Images. While users control which information and media they share within a SNS, they can't control which content other users upload and link to their profile. Images might also contain metadata including the serial number of the camera used to make the pictures.

h) Difficulty of Complete Account Deletion: Users that wish to deactivate their SNS account face difficulties to do so in most cases. On the one hand because not all comments and messages sent to other users will be deleted, and on the other hand because SNS providers keep backups of account data. Most social networking sites offer the possibility to permanently delete a user account, this features are however often hidden from users. In the case of Facebook users have to follow a special link which can only be found through a search within the Facebook support center. Also account deletions may not happen quickly.

i) Watering Hole: In January 2013, the attackers used to a new approach to make SNSs user insecure. The attack was done on Facebook. The attackers hacked a mobile developer forum and when developers visited the forum their system got infected with a MAC Trojan. This attack was not done to steal profile information or funds, but it was done to infect the system of developers. After attacks on Facebook, the same attack was done on many other companies, not only on SNS, but on their insecure sites as well.

Security threats

A) **Social Networking Spam**: As SNSs steadily grow they have become interesting targets for spammers. The use of SNS spamming software furthermore automates the process of sending unsolicited bulk messages. The Spam content can reach from advertising to Phishing messages. A study based on anonymized headers of 362 million messages exchanged by 4.2 million users of Facebook, claimed that 43 per cent of all messages analyzed were to be considered as Spam. Outlined a similar threat with context-aware spam, furthermore outlined how social networking sites can be misused to automatically profile targets of spam campaigns.

b) **Cross Site Scripting, SQL injection, Viruses and Worms**: In order that users are able to customize the design of their profiles, SNSs often provide the possibility to post HTML code or queries. Furthermore third party applications (widgets) are used to extend the functionality of SNSs and together with HTML code they state a risk for Cross-site scripting (XSS) vulnerabilities. Samy/JS.Spacehero for example was a XSS worm on MySpace, which infected more than one million profiles within the first 24 hours. A number of worms targeted other social networking sites like Facebook, MySpace, and Orkut.

c) **SNS Aggregators:** Social Aggregators offer services to integrate the data from different web services and SNSs into a single platform. Popular services include Gathera, FriendFeed, Spokeo and Secondbrain. As with all singlesign on systems, the access to multiple services (in these case SNSs) depends on only one password which if selected badly states a single point failure. These services are also used to correlate user data across different SNSs. Spokeo for example provides a charged service which aggregates data of 41 social networks with someone’s email address being the only information required. As point out, SNSs providers are trying to inhibit SNS aggregators in order to “lock-in” users to their social networking service.

Identity related threats

a) **Spear Phishing using SNSs and SN-specific Phishing**: Spear Phishing attacks aretargeted phishing attacks. The information available through SNSs is harvested by scammers and used as a basis for a spear Phishing attack. SNSs are furthermore used as a medium for carrying out the Phishing attack itself, rather than using standard Email messages. Jagatic et al. showed that social graph information can be misused to improve the success rate of phishing,

b) **Infiltration of Networks Leading to Information Leakage**: SNSs allow users to define who has access to their personal information, for example by giving access to certain ”friends“ or by defining restricted groups (networks). These are important features to improve the privacy issues of SNSs usage but once a closed network is infiltrated the protection is rendered useless and showed that cloning of user profiles could be misused to infiltrate private networks, while outlined yet another attack to infiltrate closed networks via HTTP cookie hijacking.

c) **Profile-squatting and Reputation Slander through ID Theft:** Profile-squatting is similar to domain squatting, only that instead of Internet domains persons are targeted. Fake profiles are set up in the name of someone else in order to slander her/his reputation within a certain network. Examples include the Moroccan computer engineer who set up a name of a member of the royal family, and an Italian soccer player who sued Facebook for defamation.

Social threats

a) **Stalking:** SNSs can be misused by perpetrators to contact their victims but also to gather information on them. SNSs users often disclose location data via their pictures or personal information.

b)**Cyber-bullying and grooming**: Cyber-bullying are aggressive attacks and bullying attempts carried out over the Internet, while cyber-grooming refers to attempts by adults (pedophiles) to approach minors via the web to abuse them sexually. One of the most infamous cases involving cyber-bullying, the “Megan Meier case”, led to the suicide of a teenage girl.In the Meg Meier case the perpetrator exploited the ease of setting up a fake profile, which was also used in a recent cyber-grooming case outlined possible automated social engineering attack on basis of social networking sites.

CONCLUSION

Social networking sites are particularly useful in conveying messaging about a company and its brand, but a key goal must be to ensure the integrity of the organization including its vital infrastructure. In addition, improper information disclosures must be immediately removed or sanitized so that any negative risk is appropriately mitigated.

Clearly defined policies, tools and procedures to swiftly identify and remedy issues are crucial to provide a solid base for the desired protection. As with business continuity plans, it is of vital importance to monitor, test and continually adjust these procedures and tools, as necessary. Being vigilant with exploration of vulnerabilities and adjusting to meet these challenges will help to mitigate the risks that social networks pose to an organization.

Since harmful information can be produced outside the organization, engaging searches and monitoring software tools are necessary. Companies such as Facebook, LinkedIn and Twitter provide search utilities for "Social Media Monitoring" or "listening." These tools enable searches so that organizations can ensure proper messages are being passed, and allow them to respond to negative commentary. Along with these search engines, "Social Media Monitoring Tools" can provide automated alerts, and some can be integrated with CRM packages. Integration allows alerts to be routed to Sales, Customer Service or Marketing for appropriate research or response.

REFERENCES

Kou Y., Lu C-T., S. Sirirat. Survey on Fraud Detection Techniques [Conference] // International Conference on Networking, Sensing and Contro. - USA : IEEE, 2004. - Vol. 2. - pp. 749- 754 .

Hilas C., Sahalos, J. User Profiling for Fraud Detection in Telecommunication Networks [Conferência] // 5th International Conference on Technology and Automation . - Greece : IEEE, 2005.

Adriaans P., Zantinge, D. Data Mining [Book]. - Harlo. England : Addison-Wesley, 1996.

Weatherford M. Mining for Fraud [Jornal] // IEEE Intelligent Systems. - [s.l.] : IEEE, 2002. - pp. 4--7.

Hall L. Data mining from extreme data sets: Very large and/or very skewed data sets [Conferência]. - [s.l.] : IEEE, 2001. - p. 2555.

Vo N., Won, Y. Classification of Unbalanced Medical Data with Weighted Regularized Least Squares [Conferência] // Frontiers in the Convergence of Bioscience and Information Technologies. - [s.l.] : IEEE, 2007. - pp. 347--352 .

*Lewis, K., Kaufman, J., Gonzalez, M.,Wimmer, A., Christakis, N.: Tastes, ties and time: a new social network dataset using FaceBook.com. Soc. Netw. **30**, 330–342 (2008). Elsevier*

Abraham, A., et al.: Reducing social network dimensions using matrix factorization methods. In: Proceedings of the 2009 Advances in Social Network Analysis and Mining, 19 Jan 2009, pp. 348–351. IEEE press, Piscataway (2009)

Abraham, A., et al.: Social aspects of web page contents. In: Abraham, A., Sn´asel, V.,Wegrzyn-Wolska, K. (eds.) Proceedings of the International Conference on Computational Aspects of

Social Networks, CASoN 2009, Fontainebleau, France, 24–27 June 2009, pp. 80–87. IEEE Computer Society, Washington, DC (2009)

Zhou, L., Ding, J., Wang, Y., Cheng, B., Cao, F.: The social network mining of BBS. J. Netw. ***4****(4), 298–305 (2009)*

Markus Huber, Martin Mulazzani, and Edgar R. Weippl. (2010). Who On Earth Is Mr. Cypher? Automated Friend Injection Attacks on Social Networking Sites. Security and Privacy—Silver Linings in the Cloud, 1, 80--89. http://friendinjection.nysos.net (journal article)

FANG, L. & LEFEVRE, K. "Privacy wizards for social networking sites,"Proceedings of the 19th international conference on World wide web, pp. 351-360. ACM, 2010.

LIPFORD, H. R., BESMER, A. & WATSON, J. "Understanding privacy settings in facebook with an audience view,"Proceedings of the 1st Conference on Usability, Psychology, and Security, pp. 1-8. USENIX Association Berkeley, CA, USA, 2008.

Ashwin Machanavajjhala, Daniel Kifer, Johannes Gehrke, "l-diversity: Privacy beyond k-anonymity," In: ACM Transactions on Knowledge Discovery from Data (TKDD), vol. 1, 2007.

Qiong Wei, Yansheng Lu, "Preservation of Privacy in Publishing Social Network Data", In Proc. of International Symposium on Electronic Commerce and Security, Guangzhou City, pp 421 - 425, 2008.