Social Networking Sites Security: Quo Vadis

Markus Huber*, Martin Mulazzani*, Edgar Weippl*
*SBA Research
AT-1040 Vienna, Austria
Email: {mhuber,mmulazzani,eweippl}@sba-research.org

***Abstract*—Social networking sites have been studied extensively within the past five years, especially in the area of information security. Within this paper we discuss these emerging web services both regarding possible attack vectors as well as defense strategies. Our results suggest that a gap between attack and defense strategies exists. Furthermore we found that research focuses mainly on Facebook, while scant attention is paid to other social networking sites.**

***Index Terms*—social networking sites, security, survey**

I. Introduction

A variety of social networking sites (SNSs) are used by hundreds of million users. At the time of writing Facebook is the biggest online social networking service with over 400 million active users. Users provide personal information about themselves including their interests, social relationships, current occupation, pictures and other media content, and share this information via SNSs platforms. Due to the sensitivity of information stored within social networking sites a plethora of research in the area of information security has been conducted. While there is a continual flow of media stories discussing privacy and security problems of SNSs, the great majority of academic contributions focus either exclusively on possible threats on one hand, or possible protection strategies on the other. The aim of this paper is thus to provide an introduction to both state-of-the-art attack scenarios as well as possible mitigation strategies for social networking sites, to ultimately spot potential gaps between attacks and defenses. The main contributions of this paper are:

- A summary of attack scenarios on basis of SNSs.
- Possible mitigation strategies to protect personal data within SNSs.
- A brief gap-analysis between attack and protection strategies for SNSs.

The rest of the paper is organized as follows: section II introduces social networking sites and gives an overview on related research. Section III outlines current security and privacy threats regarding social networking services. In the following, we describe possible protection mechanisms for social networking sites IV. In section V we draw conclusions from our findings.

II. Background

Social networking sites (SNSs) account to today's most popular web services. The main purpose of SNSs is to offer services to foster social relationships and tools to share media online. There exists a number of competing SNSs providers, which [11] divided into general-purpose and niche sites. While SNSs are in general accessed via web browsers, SNSs providers started to offer interfaces for access through mobile phones as well. Table I shows the most popular social networking sites on basis of their self-claimed user base.

Social networking sites have been studied in a variety of academic disciplines. Scholars from social sciences have studied impact SNSs have upon the young generation and their motives to join online social networks [12], [13], [18], [31]. Within the field of computer science, research has been conducted to quantify the size and structure of online social networks [35], [3], [23], [30]. The pool of context information aggregated by social networking sites is of high value for attackers as it is a promising source for malicious attacks. Thus social networking sites have been studied extensively within the area of information security research. Personal information forms the ideal base for social engineering, which exploits the weakest link of IT-systems: the people who are using them. A social engineer tries to manipulate her/his victims into divulging confidential information or performing her/his malicious objectives by using influence and persuasion. Because of the emerging usage of SNSs the toolset available to attackers changes, as they can now use SNSs such as Facebook to gather the initial background information on future victims (instead of phone calls or dumpster-diving). [29], [14], [27] demonstrated how context-information harvested from SNSs can be misused in order to carry out sophisticated social engineering attacks. J. Bonneau compiled an extensive bibliography [8] on security & privacy in social networking sites which is updated regularly. The bibliography is divided into 10 sub-areas (see Fig. 1) and offers in our opinion a valuable summary on research regarding social networking sites' security & privacy.

Methodology We visualized the publication trend for research in SNSs security and privacy in Fig. 1. In order to draw conclusions on a possible gap between SNSs attack and defense strategies, we decided to focus on the subcategories "Attacks" and "Privacy-enhanced architectures" (bold lines in Fig. 1) of Bonneau's online bibliography. Security threats related to social networking usage are then further outlined in section III arranged according to the categories proposed by Hogben et al. [26]. Research related to privacy and security protection mechanisms for SNSs is finally summarized in section IV.

Social Networking Site		
Name	Type	User-base
Facebook	General-purpose	400×10^6
MySpace	General-purpose	264×10^6
Qzone	General-purpose	200×10^6
Windows Live Spaces	General-purpose	120×10^6
Habbo	Niche (Gaming)	117×10^6
Friendster	General-purpose	90×10^6
hi5	General-purpose	80×10^6
Tagged	General-purpose	70×10^6
Orkut	General-purpose	67×10^6
Netlog	General-purpose	58×10^6

Table I: Ten biggest social networking sites at the time of writing based on their self-claimed number of users

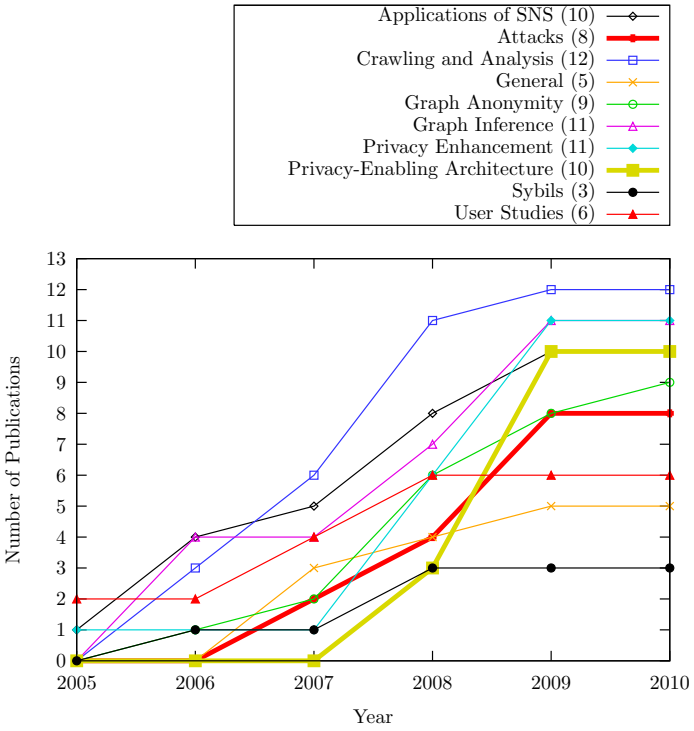

Figure 1: Scientific publications in the area of privacy & security in social networking sites. The publications are divided into different sub-areas to visualize publication trends.

III. SNSs ATTACK SCENARIOS

The ENISA[1] position paper [26] from 2007 introduced four threat categories, which offer a valuable starting point to understand the various information security risks that are involved with SNSs usage. Hence within the following section we revisit the threat categories as proposed by Hogben et al. [26] in order to estimate to which extent their scenarios became reality since the published their attack scenarios in 2007.

[1]European Network and Information Security Agency

1) 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. [26] 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 1.074.574 profiles could be aggregated within less than four hours with a computer cluster consisting of ten computers [22]. [10] highlighted various methods how data could be collected from Facebook. [9] furthermore showed that information that is publicly available could be used to infer the social graph of SNSs users. A commercial provider [1] 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 [19] 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) *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.

f) *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 an 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.

2) **SNS variants of traditional network and information 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 [24]. [14] outlined a similar threat with context-aware spam. [5] furthermore outlined how social networking sites can be misused to automatically profile targets of spam campaigns.
   b) *Cross Site Scripting, 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. 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 [38], [37], [34].
   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 single-sign-on systems, the access to multiple services (in this 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 [39]. As [11] point out, SNSs providers are trying to inhibit SNS aggregators in order to "lock-in" users to their social networking service.

3) **Identity related threats**
   a) *Spear Phishing using SNSs and SN-specific Phishing.* Spear Phishing attacks are targeted 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. [29] 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. [7] showed that cloning of user profiles could be misused to infiltrate private networks, while [28] 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 [6], and an Italian soccer player who sued Facebook for defamation [16].

4) **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 (see CBR) 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 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 [40]. 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 [42].
   c) *Corporate Espionage.* [26] discusses the threat of corporate espionage via SNSs regarding social engineering. A social engineer can use SNSs to collect valuable information about employees (employees of a specific organization, position within the organization, full name, Email addresses etc.) rather than infiltrating an organization and using classic social engineering approaches. [27] outlined

a possible automated social engineering attack on basis of social networking sites.

In summary one can observe that except of face recognition and CIBR vulnerabilities, all threats of the ENISA position paper have been either observed in-the-wild or outlined on a proof-of-concept basis by academia. One trend however has not been foreseen by the position paper, namely risks through third-party applications. Most SNSs providers started to offer developer APIs which can be used by third-parties to serve applications to SNSs users. These APIs offer a new way to tap the pool of personal information stored within social networking sites via custom applications. According to [20] the context-information given to third-party applications is usually not anonymized, even though most applications would be able to function on anonymized profiles. Additionally to the sensitive information these third-party applications can access on a large scale, a number of malicious third-party applications have been detected which e.g., serve spyware [21] and malware [36].

IV. SNSs PROTECTION STRATEGIES

Recently various data protection schemes have been proposed to protect the user's privacy in social networks against malicious or curious entities. These entities might either be the social network operator itself, someone from within the users' social context, or an external adversary who tries to use social networks as attack vector. Common methods for defense include the use of encryption, data dissociation or the usage of fake information. A combination of these methods is likely to protect the users' privacy to a larger extend. Some methods assume the cooperation of the social network operator, by including parts of the functionality in the codebase of the SNS. Others assume that there is no incentive for the operators to include any code to protect users privacy, and is even contrary to the operator's business model as they offer their service for free and make money by using the demographic information of the users for advertisements. They are designed to leave the SNS unchanged and build on top of it a layer of protection for a subset of privacy-savvy users. This will not enhance the privacy of all or the majority of users, but enables users who want to keep some of their data confidential to use the social network. In this section we present an overview of available and recently proposed techniques, and some of their shortcomings.

Encryption can be used to secure communication channels. In the most naive approach this means that the communication between the users and the social network uses encryption (e.g., HTTPS) to protect against eavesdropping. However, this from a technical standpoint simple, easy applicable and readily available protection instrument is not widely used by most of the SNSs [28]. XING is the exception, as it uses HTTPS for all client communication. Encryption can be further used to protect content distribution like user-to-user communication on the SNS without modifications to the underlying infrastructure. This defeats an honest, but curious SNS operator from eavesdropping, as well as an adversary that is able to get access to the data in any unauthorized way. Tools like the Firefox extension FirePGP [2] are readily available to encrypt and decrypt any textual information within a web browser, but lack the convenient user interface or general usability for the average user. To sum up about encryption, methods for usage with or without a cooperative social network operator exist, but are most likely too complicated or expensive for general adoption.

Data dissociation can be used to separate the amount of data stored at the SNS. All publicly available information can be stored at the SNS, while private and sensitive information could be stored at a third party e.g., the computer of the user, a trusted third party, or an untrusted third party. To protect the information at the untrusted third party, encryption can be used to allow confidentiality or fine grained access controls. *Lockr* [41] for example uses a Facebook application to provide and manage access to any external third party data within the social context of Facebook, protected from unauthorized users by means of encryption. By using zero-knowledge proofs as social attestations within their protocol, social relationships are hidden from the third party service. At the moment, only picture sharing at Flickr and BitTorrent sharing over Vuze are supported, but the scheme is theoretically applicable to any third party service. However, due to the needed implementation effort, a universal usage on a large scale will be hard to achieve although possible. *FlyByNight* [32] is another Facebook application that uses client side encryption to publish encrypted messages to the flyByNight server. The recipients then retrieve the messages and decrypt them locally, without either Facebook or any adversary listening on the line being able to decrypt the message. Encryption is done in JavaScript, which means that compared to other languages it is rather slow. The advantage of this is that there is no trusted entity or software needed for encrypting the messages except the webbrowser of the user. By using "proxy cryptography", the client side work load can be further reduced in one-to-many communications, while keeping the security properties intact. Despite the performance drawback, the threat model of flyByNight relies on Facebook not to replace JavaScript code used for cryptographic operations, which they argue is reasonable. However, an active adversary might replace code or public keys if she is able to conduct a man in the middle attack as communication with Facebook does not use HPTTS.

Fake information can be used as an additional layer of protection against curious social networking operators or external adversaries. The social network only sees the fake information, while possibly authentic and sensitive information is stored encrypted on a third party server. As a source for fake information either predefined wordlists or dynamic content from the Internet might be used. This prevents naive approaches for detecting the fake information. NOYB [25] for example shuffels user data among all

NOYB users to increase privacy, based on a cryptographic pseudorandom algorithm. It is implemented as Firefox extension and uses a public dictionary of all users as input. This means that the NOYB users can hide among all NOYB users, while it still remains relatively hard to detect and works without changing the underlying infrastructure of Facebook. The Firefox extension FaceCloak [33] on the other hand uses a slightly different approach, by using random articles from Wikipedia as source for fake data and custom wordlists as source for fake names. This provides strong privacy against Facebook and unauthorized users. Despite the fake information, encrypted real information is stored on a third party server. FaceCloak takes care of the mapping of fake data from Facebook, and encrypted information from the third party. However, in their implementation key management might pose an issue, as FaceCloak has yet no support for revoking keys. This means that if a friend "looses" a key or gives it away, the information becomes accessible to that unauthorized entities. Furthermore, a user needs access to his keys to be able to use it at a different computer.

Decentralized architectures raise a lot of technical challenges, especially in terms of availability and security. In [15] a solely peer-to-peer based approach is discussed, without a single point of failure for the data or the confidentiality of the data itself. Diaspora [17] is a recent project, aiming to build an open source, distributed and decentralised alterantive to already deployed networks. Another possible solution would be to use already well understood distributed systems like email or distributed file systems, and build social network functionality on top of them. It is unlikely from our point of view that a complete peer-to-peer based approach will be as successfull as already deployed networks in the near future, with millions of users.

Privacy as a feature or "privacy by design" might be used by future SNS to distinguish themselves from deployed SNSs, offering privacy to attract more users. It is unlikely that operators that generate revenue by using private information will add such contrary services. To offer the users a customizable degree of privacy they rely on user-generated access control policies and enforce them by means of cryptography. This guarantees that only authorized users or applications are able to access sensitive information. Persona [4] uses a combination of attribute-based cryptography and public key cryptography to protect information. This allows neat features like encrypted group messages without needing to know the entire list of group members, or the need for encrypting the message with the public key of every member in the group. No trust has to be put on the service operators that store the data, or on the application providers (every service in Persona is implemented as an application). They also offer their software to use it on top of Facebook as a third party application in combination with a Firefox extension. However, care has to be taken that the average user is not overstrained by too many technical details or security choices. The user interface needs to be as simple as possible, while at the same time allowing fine grained access policies. It is important for the future to raise the awareness of possible privacy impacts by using social networks, to make people realize that their data is at risk.

Stenography might be used to embed information in pictures or videos hosted or exchanged over SNS. As the videos and pictures are transformed upon submission to fit the size constraint of the websites, the steganographic algorithms need to be robust enough to withstand these transformations. NOYB [25] for example relies on stenography as one possible communication channel.

V. Conclusion

Within this paper we examined both attack and protection strategies for social networking sites. A number of practical attacks have been outlined by researchers in the last five years and a fast number of actual attacks have been observed in-the-wild. Given the emerging threats of social networking usage we hence explored mitigation strategies for these attacks. We divided protection mechanisms into four subgroups: encryption, data dissociation, fake information, and privacy as a feature. Stenography might be used in combination with any of the other subgroups, to further increase stealthiness. The most promising defense strategies in our understanding are fake information and "privacy as a feature" respectively "privacy by design". While fake information is a very effective countermeasure which could also help to mitigate sophisticated social engineering attacks such as social phishing, the approach does not scale. Fake information and data dissociation approaches rely upon third-party storage and e.g. in the case of Facebook with over 400 million users, fast resources would be needed to provide all users with such an additional protection layer. Hence social networking services which are designed from scratch with a focus on information privacy and security might effectively counter state-of-the-art attacks and scale at the same time. What is missing in our opinion are business models for "privacy as a feature" systems which could make these alternative systems a reality. These novel systems would furthermore have to overcome "lock-in" effects which currently hinder users from migrating their user data from one SNSs provider to another. In summary we observed a gap between current attacks and defenses which has to be tackled with new protection mechanisms. Finally we found that current research almost exclusively focuses on Facebook as it is the biggest of all networks, and other social networking sites are often neglected.

References

[1] 80legs. http://80legs.com/.

[2] Firegpg browser extension. http://getfiregpg.org/.

[3] Y.Y. Ahn, S. Han, H. Kwak, S. Moon, and H. Jeong. Analysis of topological characteristics of huge online social networking services. In *Proceedings of the 16th international conference on World Wide Web*, page 844. ACM, 2007.

[4] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: An online social network with user-defined privacy. *ACM SIGCOMM Computer Communication Review*, 39(4):135–146, 2009.

[5] M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, and C. Kruegel. Abusing Social Networks for Automated User Profiling. 2010.

[6] BBC News. Jail for Facebook spoof Moroccan. online, 2008. [Retrieved 2008-12-01].

[7] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda. All your contacts are belong to us: Automated identity theft attacks on social networks. In *18th International World Wide Web Conference*, April 2009.

[8] J. Bonneau. Security and Privacy in Social Networks Bibliography. online, 2010. [Retrieved 2010-05-10].

[9] J. Bonneau, J. Anderson, R. Anderson, and F. Stajano. Eight friends are enough: social graph approximation via public listings. In *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, pages 13–18. ACM, 2009.

[10] J. Bonneau, J. Anderson, and G. Danezis. Prying data out of a social network. In *First International Conference on Advances in Social Networks Analysis and Mining*, 2009.

[11] J. Bonneau and S. Preibusch. The Privacy Jungle: On the Market for Privacy in Social Networks. In *Eighth Workshop on the Economics of Information Security (WEIS)*, 2009.

[12] D. Boyd. Why Youth (Heart) Social Network Sites: The Role of Networked Publics. *Teenage Social Life. Youth, Identity and Digital Media. MIT Press, Cambridge, MA*, pages 119–142, 2007.

[13] D.M. Boyd and N.B. Ellison. Social network sites: Definition, history, and scholarship. *JOURNAL OF COMPUTER MEDIATED COMMUNICATION-ELECTRONIC EDITION-*, 13(1):210, 2007.

[14] G. Brown, T. Howe, M. Ihbe, A. Prakash, and K. Borders. Social networks and context-aware spam. In *Proceedings of the ACM 2008 conference on Computer supported cooperative work*, pages 403–412. ACM New York, NY, USA, 2008.

[15] S. Buchegger, D. Schiöberg, L.H. Vu, and A. Datta. PeerSoN: P2P social networking: early experiences and insights. In *Proceedings of the Second ACM EuroSys Workshop on Social Network Systems*, pages 46–52. ACM, 2009.

[16] cnet news cnet news. Italian soccer star to sue facebook, 2009. [Online; accessed 22-March-2010], http://news.cnet.com/8301-17852_3-10159147-71.html.

[17] Diaspora. Diaspora, 2010. [Online; accessed 1-March-2010], http://www.joindiaspora.com/.

[18] C. Dwyer. Digital relationships in the" myspace" generation: Results from a qualitative study. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pages 19–19, 2007.

[19] EFF. Some lessons from the at&t/facebook switcheroo, 2010. [Online; accessed 10-March-2010], http://www.eff.org/deeplinks/2010/01/some-lessons-att-facebook.

[20] A. Felt and D. Evans. Privacy protection for social networking APIs. *2008 Web 2.0 Security and Privacy (W2SP'08)*, 2008.

[21] FortiGuard. Facebook widget installing spyware, 2008. [Online; accessed 25-March-2010], http://www.fortiguard.com/advisory/FGA-2007-16.html.

[22] Hagen Fritsch. StudiVZ - Inoffizielle Statistiken vom Dezember 2006. online, 2008. [Retrieved 2008-11-29].

[23] M. Gjoka, M. Kurant, C.T. Butts, and A. Markopoulou. A walk in Facebook: Uniform sampling of users in online social networks. In *Proc. of the IEEE Infocom*, 2010.

[24] S. Golder, D.M. Wilkinson, and B.A. Huberman. Rhythms of social interaction: messaging within a massive online network. *Arxiv preprint cs.CY/0611137*, 2006.

[25] S. Guha, K. Tang, and P. Francis. NOYB: Privacy in online social networks. In *Proceedings of the first workshop on Online social networks*, pages 49–54. ACM, 2008.

[26] G. Hogben. Security Issues and Recommendations for Online Social Networks. *Position Paper. ENISA, European Network and Information Security Agency*, 2007.

[27] Markus Huber, Stewart Kowalski, Marcus Nohlberg, and Simon Tjoa. Towards automating social engineering using social networking sites. *Computational Science and Engineering, IEEE International Conference on*, 3:117–124, 2009.

[28] Markus Huber, Martin Mulazzani, and Edgar Weippl. Who on earth is "mr. cypher": Automated friend injection attacks on social networking sites. In *Proceedings of IFIP/SEC 2010*, 2010. to appear.

[29] T.N. Jagatic, N.A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Communications of the ACM*, 50(10):94–100, 2007.

[30] R. Kumar, J. Novak, and A. Tomkins. Structure and evolution of online social networks. In *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, page 617. ACM, 2006.

[31] S. Livingstone. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3):393, 2008.

[32] M.M. Lucas and N. Borisov. flybynight: Mitigating the privacy risks of social networking. In *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, pages 1–8. ACM, 2008.

[33] W. Luo, Q. Xie, and U. Hengartner. FaceCloak: An Architecture for User Privacy on Social Networking Sites. In *Computational Science and Engineering, 2009. CSE'09. International Conference on*, volume 3, 2009.

[34] Trend Micro. New variant of koobface worm spreading on facebook, 2009. [Online; accessed 14-March-2010], http://blog.trendmicro.com/new-variant-of-koobface-worm-spreading-on-facebook/.

[35] A. Mislove, M. Marcon, K.P. Gummadi, P. Druschel, and B. Bhattacharjee. Measurement and analysis of online social networks. In *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, page 42. ACM, 2007.

[36] SophosLabs. Farm town virus warning: Malvertising at work?, 2009. [Online; accessed 5-April-2010], http://www.sophos.com/blogs/gc/g/2010/04/12/farm-town-virus-warning.

[37] SophosLabs. Large scale orkut virus outbreak not cool, 2009. [Online; accessed 12-March-2010], http://www.sophos.com/blogs/sophoslabs/v/post/900.

[38] SophosLabs. Xss worm targeting chinese website, 2009. [Online; accessed 12-March-2010], http://www.sophos.com/blogs/sophoslabs/v/post/6208.

[39] Spokeo. Spokeo/hr - Explore beyond the resume. online, 2008. [Retrieved 2008-12-01].

[40] Suburban Journals. 'My Space' hoax ends with suicide of Dardenne Prairie teen. online, 2008. [Retrieved 2008-11-28].

[41] A. Tootoonchian, S. Saroiu, Y. Ganjali, and A. Wolman. Lockr: better privacy for social networks. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, pages 169–180. ACM, 2009.

[42] Chicago Tribune. Facebook child porn case results in 35-year federal prison term. online, 2008. [Retrieved 2008-11-29].