Re-Socializing Online Social Networks

CONFERENCE PAPER · JANUARY 2011

DOI: 10.1109/GreenCom-CPSCom.2010.18 · Source: IEEE Xplore

Martin Werner
Ludwig-Maximilians-University of Munich

2010 IEEE/ACM International Conference on Green Computing and Communications & 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing

Re-Socializing Online Social Networks

Michael Dürr
Mobile and Distributed Systems Group
Department for Informatics
Ludwig-Maximilians-University
80538 Munich, Germany
Email: michael.duerr@ifi.lmu.de

Martin Werner
Mobile and Distributed Systems Group
Department for Informatics
Ludwig-Maximilians-University
80538 Munich, Germany
Email: martin.werner@ifi.lmu.de

Marco Maier
Mobile and Distributed Systems Group
Department for Informatics
Ludwig-Maximilians-University
80538 Munich, Germany
Email: maierma@cip.ifi.lmu.de

***Abstract*—At present, the rapid development of *Online Social Networks* (OSN) has strong influence on our global community's communication patterns. This primarily manifests in an exponentially increasing number of users of *Social Network Services* (SNS) such as Facebook or Twitter. A fundamental problem accompanied by the utilization of OSNs is given by an insufficient guarantee of its users' informational self-determination and the dissemination of socially intolerable content. This results in severe shortcomings for both the possibility to customize privacy and security settings as well as the unsolicited centralized data acquisition and aggregation of profile information and personal content.**

In this paper we provide an analysis of requirements an OSN has to fulfill in order to guarantee compliance with its users' privacy and security demands. Furthermore, we present a novel decentralized multi-domain OSN design which complies with our requirements. This work significantly differs from existing approaches since it provides a technically mature mapping of real-life communication patterns to an OSN. Our concept represents the basis for a secure and privacy-enhanced OSN architecture which eliminates the problem of socially intolerable content dissemination.

I. Introduction

Online Social Networks (OSNs) offer means to map communication flows of real-life relationships to existing computer networks such as the Internet. Almost all successful *Social Network Service* (SNS) providers like LinkedIn, MySpace, Facebook, Twitter, and others, operate their services commercially and in a centralized way. Although many of these SNSs address selected user groups (LinkedIn targets at business professionals, MySpace primarily addresses private relationships), they all have in common that their users utilize these OSNs for communication, information sharing, and data exchange.

SNSs provide a convenient way to shift a multitude of everyday communication, information access, and information retrieval operations to a single, centralized platform. The increasing number of OSN memberships reflects their immense popularity. Facebook alone grows at a rate of over 700.000 users a day [1] and currently holds 400 million active users, i.e. users who have returned to the site in the last 30 days [2]. However, convenient communication and information sharing gives rise to serious concerns with regard to a user's *informational self-determination*. In general, user data is concentrated under one single administrative domain, and therefore, is subject to both intentional as well as unintentional data disclosure. Of course, there are users who do not care about the disclosure of their profile data as they maintain and operate their OSN account for profiling purposes or even as an avatar. Nevertheless, plenty of users trust SNS providers to comply with their privacy and security statements ignoring the fact that no provider can guarantee for the integrity of the software system and all of its employees.

In contrast to such user preferences, many SNS providers attempt to aggregate centrally stored users' profile information to map and link their social dependencies to one *social graph*. A social graph represents an extremely valuable knowledge base which allows for data mining operations such as the derivation of individual preferences and habits. For instance, such data could be utilized by third party providers in order to realize personalized recommendation systems. Facebook's *social plugins* [3] enable such recommendations as they permit third party providers to query Facebook by means of the *Open Graph Protocol* [4] for profile information in order to enrich their website with personalized content. An even worse situation is given in case an insurance company derives knowledge about a user's sport activities, food patterns, or even personal indispositions from a social graph. This information could be abused to estimate health hazards and risks for illness in order to increase costs for the insured.

Since every SNS provider guarantees strict adherence to its users' privacy requirements, one might argue that in reality such threats do not exist. However, recent past has shown that the threat of data leaks [5], [6] as well as the unsolicited relaxation of OSN privacy settings [7]–[9] cannot be prevented. Even profile deletion represents a serious problem. Although most OSN providers offer the opportunity to terminate accounts, such a termination does not necessarily mean that each post or upload to an OSN will dissolve [10]. Such content can distribute to other sites and is no longer under its author's control [11].

OSNs greatly support the distribution of any content (documents, email, photos, forum threads, . . .) on the Internet. As a result, a user loses control over his content as soon as he releases it [12]. Hence, a multitude of users not only suffer from the threat of unsolicited profile disclosure and private data leakage, but also from *social network pollution*. This must be attributed to sizable contact lists which often comprise several hundred contacts per user [2]. This increase is mainly driven

978-0-7695-4331-4/10 $26.00 © 2010 IEEE
DOI 10.1109/GreenCom-CPSCom.2010.18

by the fact that anybody is allowed to offer his friendship to anybody else. Often such invitations are accepted without expressive knowledge of its originator. Personal information and content becomes available to a multitude of questionable contacts, a development, a user should never intend.

Focusing on aspects of mobile computing, we identify another problem users presently suffer from. A multitude of SNS and third party providers already offer context-aware applications for *Mobile Internet Devices* (MID). Such applications allow for the interaction with nearby users supported by profile information collected from an OSN. However, none of these software solutions support anonymous and secure contextualized communication, information aggregation, and information provision. The authors of [13] present a framework to enrich real-world location-based services (LBS) with social network information without compromising user privacy and security. The proposed architecture allows to query a local area for social network information without disclosing a mobile user's identity. However, their solution does not solve privacy and security concerns, but shifts responsibility for sensitive data to a trusted third party.

In this paper, we present a hybrid and decentralized OSN design which aims on maximum compliance with user privacy and security. At the same time, our approach allows for minimal OSN pollution through undesirable linkage of users. The main contributions of this work are *a)* a requirements analysis to support strong privacy and security for OSNs, *b)* a novel multi-domain design for a highly-available and decentralized OSN which complies with the elaborated requirements and *c)* a technical transformation of real-life communication patterns to an appropriate social network messaging design.

The rest of this paper is organized as follows. Section II provides a requirements analysis which forms the basis for our OSN design. A scheme for secure communication and a detailed description of the multi-domain OSN design are given in section III. The technical transformation and integration of real-life communication patterns into our design are detailed in section IV. Section V discusses related work before section VI concludes the paper.

II. Requirements

There exist several requirements every OSN must meet. In this work we focus on security and privacy demands. Though SNS providers made some effort to comply with privacy demands, applications such as *WhosHere* [14] or *Loopt* [15] render them useless. Both share social network identifiers over short range communication interfaces (Bluetooth, WiFi) and hence are able to aggregate a user's profile information. Furthermore, these systems enrich that aggregation with location information and technical details such as a MAC-address. Such an aggregation results in even worse personal profile disclosure. In order to better understand the imminent necessity to turn away from present OSN designs, we define a set of requirements SNSs should adhere to in order to *a)* better match the intention of an OSN being a platform for private communication according to real-life communication patterns and to *b)* allow for secure and privacy-preserving data distribution and communication.

A. Informational self-determination

A centralized administration of OSN profiles and uploaded content is incompatible with a user's demand for informational self-determination. Even in case a trusted third party guarantees secure and confidential access to this data, the problem of centralized administration still exists. A completely anonymous and decentralized OSN must not allow for centralized hosting of sensitive data as well as for the reliance on any kind of third party at all. Informational self-determination requires that neither the user profile nor personal content may be disclosed to anybody else than one's trusted contacts. A trusted contact may have any means to determine a user's present physical anchor point in order to establish a confidential communication channel. All communication must guarantee security against man-in-the-middle attacks. It must be possible for a user to configure fine-grained access to his profile information. Therefore we need a manageable and secure mechanism to publish a selected set of profile attributes, dependent on a trusted contact's identity. To give a user full control over his personal data, the possibility to permit flexible and selective profile access requires a simple and efficient revocation mechanism. This also includes the choice to terminate the own OSN account and deny future access to once published content.

B. Strong trust relationships

None of the present OSN architectures reflects that kind of social relationships we are used to maintain in reality. This must be attributed to the non-solicitous addition of unacquainted contacts and thoughtless disclosure of personal information. The process of establishing a new contact inside an OSN differs considerably from that in real life. In real life, trust heavily depends on the degree of acquaintance which is closely related to social links of a social graph. For instance, in case a best friend B of person A recommends one of his best friends C, A and B do not necessarily share the same degree of trust for C. Mapping these relationships to a social graph, B represents a *one-hop relationship* of A whereas C (given that C is not a friend of A) corresponds to a *two-hop relationship* of A. It is rather questionable whether a person A shows C any trust at all in case the shortest path between A and C is not a direct link. We will use the term *chain of trust* to refer to all vertices on a path between two users X and Y (both included) inside a social graph.

We believe that it is the process of incautiously making friends which causes huge contact lists, unsolicited profile and personal information dissemination, and associated network pollution in an OSN. As a major requirement, we limit the maximum length of the chain of trust to one-hop relationships. As a result, it becomes almost impossible to arbitrarily search the OSN for unacquainted contacts. Nevertheless, a user should still be able to get into contact with his two-hop relationships. It should be stressed that the process of contacting a two-hop relationship must not violate the previously elaborated requirements for informational self-determination. Hence, a user A must not publish profile information of his one-hop relationship$B$ as this would violate B's informational self-determination.

C. Profile availability

To prevent social graph construction and abuse, it is indispensable to turn from a centralized to a decentralized OSN architecture. Even a trusted third party cannot guarantee the requirement of informational self-determination as defined before. A decentralized infrastructure which complies with our demands requires each participant to administer his profile on his own. However, an OSN is worth nothing if published profile information is not accessible at any time. Hence, we need the possibility for secure and privacy-preserving online publication and storage to allow access to data while its owner is offline. Consequently, we insist on permanent availability and authenticated accessibility of all profile information even in case the corresponding user is offline.

D. Mobility support

To allow for context-aware and intelligent applications a modern OSN needs special support for mobile devices which, at present, suffer from limited bandwidth, computing power, and problems with complex user interfaces.

III. Concept and Design

Due to the requirements identified in section II, we decided to separate our architecture into three domains: a *social webspace*, a *social mobilespace*, and a *social homespace* (see figure 1). Our design distinguishes between synchronous and asynchronous communication. The mechanism for message exchange between entities of the social mobilespace and the social homespace allows for secure and asynchronous messaging between acquainted users. According to [16], we chose modern technologies such as strong encryption and some sort of microblogging to enable anonymous information exchange between users. The social webspace is a passive system component and represents the access point for identity information of a user. Amongst others, this location holds information about a user's name, mailing address, email address, and age. To limit profile access to the owner and his one-hop relationships only, this information is stored in a strongly encrypted way. The social homespace represents one of possibly many computing devices like a personal PC which provide access to an OSN. The social homespace differs from any other device in that it is allowed to modify a user's social webspace. The social homespace is responsible for the maintenance of a user's profile data as well as profile copies and associated cryptographic keys of his one-hop relationships. The social mobilespace corresponds to any kind of MID a user can optionally register with the social homespace. A registration may result in proactive notifications in case the social homespace experiences profile updates. Although social homespace and social mobilespace significantly differ, it should be transparent to a user and his one-hop relationships whether he is interfacing the OSN through his social homespace or his social mobilespace.

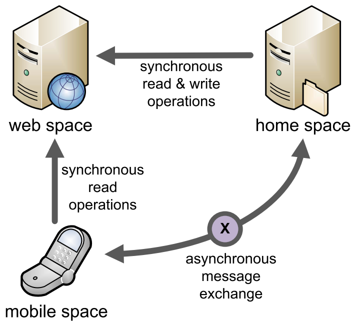

Fig. 1. User-centric visualization of the OSN domains. Entities of the social mobilespace are restricted to (synchronous) read-only operations on the social webspace. The social homespace has (synchronous) read and write permissions. Message exchange between social mobilespace and social homespace is bidirectional, asynchronous, and based on the concept of exchangers.

A. Secure Messaging

Since message exchange between users of an OSN requires asynchronous communication, we decided to model our messaging scheme as an abstract channel which provides similar functionality as a mailbox. The proposed OSN messaging mechanism adopts the idea for *locagram* exchanges as described in [16]. Assuming an already established one-hop relationship, two users A and B possess a *link-specific* public key pair for exclusive communication with each other. A is the only OSN participant which knows about the public key B has generated for exclusive communication with A and vice versa. The reason for our decision to generate a separate key pair for each directed edge of the underlying social graph is twofold: First, we achieve a reasonable degree of anonymity since it becomes computational expensive to derive a user's identity from its social link-specific public keys. Second, in case a public key is considered *compromised*, revocation can be simply performed by deleting the corresponding private key. A public key is considered to be compromised in case any user C determined the identity of its creator.

Besides the link-specific public key, A knows about an address of the link-specific communication channel, called *exchanger*, which provides the functionality of a mailbox for B. Such an exchanger could be realized through non-persistent technologies (e.g. IRC), semi-persistent public storage such as a microblog (e.g. Twitter), or fully persistent technologies (e.g. WebDAV). Hence, an exchanger could be addressed by a nickname, a channel name, or an URL. In case A wants to send a message to B, A encrypts its message based on B's link-specific public key (e.g. in accordance to PGP [17]) and places the encrypted message together with the corresponding public key at B's link-specific exchanger. B can then fetch and decrypt all messages sent to his exchanger. It should be stressed that a user can utilize multiple exchangers. In order to increase the computational complexity to determine identities, a user can decide to announce a separate exchanger to each of his one-hop relationships.

B. Social Webspace

The social webspace may be seen as a directory service which provides information about a user to his one-hop relationships. Due to the requirement for profile availability, the social webspace must be always online. Since the social homespace and social mobilespace cannot guarantee permanent availability, it must be possible to export this component to a third party webspace provider. Following our requirement for strong trust relationships, as a default, we deny unencrypted publication of any kind of personal as well as one-hop relationships' information. The social webspace holds profile information encrypted for each one-hop relationship based on the corresponding link-specific public key. Furthermore, it stores one-hop relationship exchanger addresses for each entity (MID) of the own social mobilespace domain, again based on the corresponding link-specific public key.

To support distinct access rights for different sets of users, we encrypt one copy of the corresponding profile information for each one-hop relationship. In case of profile modifications, this necessitates re-encryption and re-publication of the profile. However, we believe that this overhead is acceptable: In our privacy-enhanced OSN architecture the threat of OSN pollution no longer exists, and hence, a user maintains a severely reduced set of one-hop relationships i.e. profiles are not subject to frequent changes. In accordance to PGP, a profile could contain symmetric group keys for a specific application like a pinboard. In this case an asymmetric operation would only have to be performed, in case a one-hop relationship has to be revoked.

C. Social Homespace

The social homespace corresponds to a personal computing environment. Although it should be transparent to a user whether he is interfacing the OSN through the social homespace or the social mobilespace, the social homespace represents the domain that has full read and write permission to access the social webspace. The social homespace has to perform an update on the social webspace in case profile changes or modifications of a one-hop relationship's access rights occur. Such an update comprises the re-deployment of all re-encrypted modifications. This also necessitates an additional synchronization routine between social homespace and social mobilespace in order to keep a user's devices synchronized.

Dependent on its configuration, the social homespace not only serves as a communication interface, but also as a personal storage for sharing content with the OSN. The social homespace could consists of a personal desktop computer, a NAS device, and a ADSL-router. To achieve communication between a user's one-hop relationships and his social homespace, the social homespace must be addressable from the Internet. Hence, a user's upstream network access device must allow for cone-NATed communication. To deny unauthorized access, personal content must be subject to access control which reflects the trust relations published in the social webspace.

D. Social Mobilespace

The social mobilespace is deployed at one or more of a user's MIDs. At present, it is very common that a mobile network provider does not assign public IP addresses to mobile phones. Proactive establishment of a channel with a device from the social mobilespace domain necessitates the knowledge about the address of a VPN-tunnel endpoint which tunnels all traffic to the corresponding device. As such a design does not comply with our demand for mobility support, we decided to map our messaging infrastructure onto the exchanger concept. As it should be transparent whether a user interfaces the OSN through the social homespace or the social mobilespace, both domains are subject to synchronization. To keep our design simple, we decided to restrict some modifications of the social webspace to the social homespace. In case the social homespace recognizes a pending update operation, it simply performs necessary write-operations to the social webspace. To keep the social mobilespace in sync with the social homespace, a user interfacing the OSN through his social mobilespace performs an interval-based read operation on his social webspace. To synchronize pending modifications from the social mobilespace with the social homespace, the corresponding device utilizes our abstract channel. As soon as the social homespace becomes active, it has to apply these modifications to the social webspace.

IV. Social Network Messaging

We decided to support two basic schemes to get into contact with another user, *a) out-of-band invitation* and *b) coupling*.

A. Out-of-band invitation

To establish a one-hop relationship between two users A and B, our design provides an email-based out-of-band (OOB) mechanism. This mechanism can be easily mapped to other OOB channels e.g. based on NFC, Bluetooth, or QR-Codes between two mobile devices. An OOB channel is needed to safely authenticate each other, i.e. to satisfy our demand for strong trust relationships. The mechanism works as illustrated in figure 2. Users A and B agree on a password or a PIN (e.g. via phone). Then A sends an E-Mail to B (1) containing a link to the OSN software, an exchanger address, a link-specific public key, and some explanatory text. This message may be seen as a weak authentication of A, as we rely on email, a personal message, and well-established email spam filter mechanisms. To achieve complete safety against spoofing and replying of email messages, one could rely on secure end-to-end email. In case B is not a member of the OSN yet, B can follow the provided link and download/install the OSN software first. After B has started the software, the technical information included in A's email invitation (exchanger address and link-specific public key) can

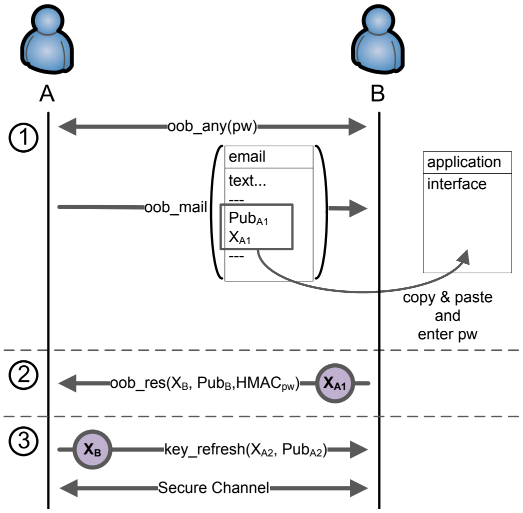

Fig. 2. Message exchange for out-of-band invitations.

be copied to the corresponding dialog. To support copy-and-paste, the invitation complies to an application-specific and e-mail compatible format. B will be prompted for the password in order to verify the request. Now B can send a message to A including a new link-specific public key, an exchanger address, and a secure message authentication code (HMAC) which is inferred from the password (2). As the link-specific public key in the email cannot be considered to be secure, A will perform a key refresh operation (3) via the secure channel established in (2). A and B have completely prepared for secure communication. Email-based invitation is a special form of OOB invitation. E.g. in a NFC-based OOB invitation, step (1) would be performed in a secure environment without the threat of spoofing or replying attacks.

B. Coupling

In reality, it is a common situation that, after a person A has introduced two of his friends B and C to each other, B and C also establish a friendship. Coupling is a simple mechanism which supports the establishment of a new one-hop relationship between two users B and C which maintain a two-hop relationship via user A in advance. Figure 3 illustrates the simplified message exchange. To initiate coupling between B and C, A sends both of them a coupling request. The request contains parts of the profiles of B and C that they have marked as public (1). In case B and C accept A's offer, each specifies a link-specific public key and an exchanger address to be used during coupling. After A received both responses, A forwards the re-encrypted messages (2). In order to comply with strong trust relationships B and C have to perform a key refresh (3) since A knows about the link-specific public keys applied during the coupling procedure. Now it depends on the trust between A and B and B and C whether a key refresh on the insecure channel can be trusted without another OOB information prohibiting A from acting as a man-in-the-middle. The idea behind the coupling mechanism is the idea of organizing groups by a virtual network participant taking the role of A.

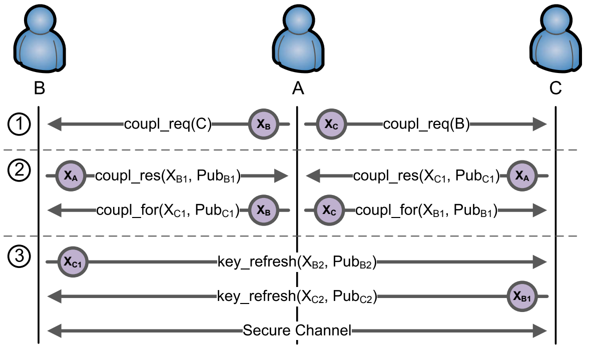
B
A
C
1
coupl_req(C)
X_B
X_C
coupl_req(B)
2
X_A
coupl_res(X_{B1}, Pub_{B1})
coupl_res(X_{C1}, Pub_{C1})
X_A
coupl_for(X_{C1}, Pub_{C1})
X_B
X_C
coupl_for(X_{B1}, Pub_{B1})
3
X_{C1}
key_refresh(X_{B2}, Pub_{B2})
key_refresh(X_{C2}, Pub_{C2})
X_{B1}
Secure Channel

Fig. 3. A initiates the coupling of B and C.

V. Related Work

The idea to migrate from centralized to decentralized and personally operated OSNs is quite young. Notable work has been published by Cutillo et al. [18], [19], who present their OSN platform Safebook. Safebook is a decentralized P2P-based architecture which targets at users that request for compliance with their personal privacy and security demands. However, since their approach depends on a DHT substrate, the authors cannot guarantee a 100% availability. A DHT also implicates additional management: it complicates the OSN protocol, it introduces additional signaling traffic, it cannot be operated without caching, and it suffers from a weaker trust model. In order to prevent well-known impersonation and sibyl attacks [20], their approach necessitates a certificate authority (CA). However, a CA again represents a centralized third party instance, which users of a decentralized OSN will not accept. The authors state that this may be implemented offline, but do not explain how. In addition, any node may request access to a user's social network information (profile). This allows for indirect friendship requests that represents the foundation for OSN pollution. Safebook also introduces a new order of complexity. To guarantee an uninterrupted chain of trust, each request forward requires message decryption, signature re-calculation, and message re-encryption. Similar to our approach, profile attributes are published encrypted. However, access in their scheme is group based, i.e. key revocation an redistribution accounts for the notification of all friends about a new key for the freshly encrypted attribute. The authors of [21] present PeerSoN, a P2P-based OSN system, that aims on privacy and security issues like authentication, encryption, and the prevention of impersonation attacks. Peers need not be connected to the Internet to make use of their social network. However, this is restricted to insight communication with other PeerSoN enabled devices and does not hold for users that want to access other profiles. Since their system offers a DHT-based lookup service, previously discussed problems still exist. Another assumption made by the authors is the availability of a GUID (e.g. an email address). In privacy enhanced networks it should be the user's choice to publish his email address or not. Even hashing does not assure complete anonymity. A node that issues recurring requests for one and the same hash could derive certain information about a user. The authors of [22] do not develop a completely novel OSN architecture, but attempt to integrate some privacy features into present SNSs like Facebook. They propose an anonymity scheme which builds on pseudo-random substitution. Based on dictionaries, each piece of encrypted data becomes substituted by a pseudo-random cipher. This approach shares our idea to encrypt little pieces of information instead of an entire profile. However, considering their proposed key management, it becomes obvious that their scheme depends on an additional channel like a trusted third party's PKI to allow for sufficient security. The authors of [23] and [24] follow a DHT-based organization of social information. However, their concept of virtual individual servers (VIS) does not meet the privacy and security demands of a decentralized OSN as administrative tasks are shifted from the centralized OSN to a centralized VIS provider. Lockr [25] targets at the improvement of privacy for centralized and decentralized online content sharing services. To some degree, this system shares some similarities with our approach since it distinguishes between the management of social relationships and shared content. It aims on enhancing privacy and accelerating content sharing. However, Lockr only reduces the chances for mismanagement or accidental disclosure of social networking information. Compared to our approach, Lockr still allows users to map content which is shared among traditional OSNs like Facebook to their anonymous OSN identity. Although each platform is mapped to a pseudonym, it is possible to correlate pseudonyms by usage and activity analysis. This allows for the collection of information about one and the same user in different OSNs. Our solution prevents such attacks as content is always hosted encrypted or can only be downloaded in case a secure session has been established in advance.

VI. Conclusion

In this paper we presented a requirements analysis for a secure and privacy-enhanced OSN. With these requirements in mind, we developed a novel OSN design which is based on the separation of an OSN into the three domains *social webspace*, *social homespace*, and *social mobilespace*. This distinction as well as the decentralized administration of all domains allows for strict compliance with our demands for permanent *profile availability* and *mobility support*. In addition, our implementation for the establishment of new relationships ensures adherence with our requirements for *informational self-determination* and *strong trust relationships*.

Thanks to the increase of computational power and storage on the Internet and Mobile Internet Devices, it is possible to utilize strong cryptographic algorithms to allow for secure information exchange. In combination with the increasing number of always-online infrastructures in the private area, it is possible to remove the need for a central platform. As this process is still ongoing, we propose to use a web-server to mirror encrypted information of the social homespace. This ensures that the social network will work as expected even in case of a disconnected social homespace.

References

[1] J. Smith, "Facebook now growing by over 700,000 users a day, and new engagement stats," July 2009. [Online]. Available: http://www.insidefacebook.com/2009/07/02/facebook-now-growing-by-over-700000-users-a-day-updated-engagement-stats/

[2] Facebook, "Press room," April 2010. [Online]. Available: http://www.facebook.com/press/info.php?statistics

[3] B. Taylor, "The next evolution of facebook platform," April 2010. [Online]. Available: http://developers.facebook.com/blog/post/377

[4] Facebook, "Open graph protocol," Mai 2010. [Online]. Available: http://developers.facebook.com/docs/opengraph

[5] T. H. Security, "Facebook fixes data leak," July 2008. [Online]. Available: http://www.h-online.com/security/news/item/Facebook-fixes-data-leak-736509.html

[6] J. V. Grove, "Blippy users credit card numbers exposed in google search results," April 2010. [Online]. Available: http://mashable.com/2010/04/23/blippy-credit-card-numbers/

[7] K. Bankston, "Facebook's new privacy changes: The good, the bad, and the ugly," December 2009. [Online]. Available: http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly

[8] R. Needleman, "How to fix facebook's new privacy settings," December 2009. [Online]. Available: http://news.cnet.com/8301-19882_3-10413317-250.html

[9] N. Carlson, "Warning: Google buzz has a huge privacy flaw," February 2010. [Online]. Available: http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2#click-into-buzz-on-gmail-1

[10] C. Walters, "Facebook's new terms of service: "we can do anything we want with your content. forever."," February 2009. [Online]. Available: http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html

[11] B. Krishnamurthy and C. E. Wills, "On the leakage of personally identifiable information via online social networks," in *WOSN '09*. ACM, 2009, pp. 7–12.

[12] B. Schneier, "Architecture of privacy," *IEEE Security & Privacy*, vol. 7, no. 1, p. 88, 2009.

[13] A. Beach, M. Gartrell, B. Ray, and R. Han, "Secure socialaware: A security framework for mobile social networking applications," Department of Computer Science, University of Colorado at Boulder, Tech. Rep. Technical Report CU-CS-1054-09, June 2009.

[14] myRete, "Whoshere," May 2010. [Online]. Available: http://myrete.com/whoshere.html

[15] Loopt, "Loopt," May 2010. [Online]. Available: http://www.loopt.com/

[16] M. Werner, "A privacy-enabled architecture for location-based services," in *MobiSec'10*, 2010.

[17] S. Garfinkel, *PGP: Pretty Good Privacy*. O'Reilly, November 1994.

[18] L. A. Cutillo, R. Molva, and T. Strufe, "Privacy preserving social networking through decentralization," in *WONS'09*. IEEE Press, 2009, pp. 133–140.

[19] ——, "Safebook: Feasibility of transitive cooperation for privacy on a decentralized social network," in *WOWMOM*, 2009, pp. 1–6.

[20] G. Urdaneta, G. Pierre, and M. van Steen, "A survey of DHT security techniques," *ACM Computing Surveys*, 2009.

[21] S. Buchegger, D. Schiöberg, L. H. Vu, and A. Datta, "PeerSoN: P2P social networking - early experiences and insights," in *Proceedings of the Second ACM Workshop on Social Network Systems 2009*, 2009.

[22] S. Guha, K. Tang, and P. Francis, "Noyb: privacy in online social networks," in *WOSP '08*. ACM, 2008, pp. 49–54.

[23] A. Shakimov, H. Lim, L. P. Cox, and R. Caceres, "Vis-à-vis:online social networking via virtual individual servers," Duke University, Tech. Rep., May 2008.

[24] A. Shakimov, A. Varshavsky, L. P. Cox, and R. Cáceres, "Privacy, cost, and availability tradeoffs in decentralized osns," in *WOSN '09*. ACM, 2009, pp. 13–18.

[25] A. Tootoonchian, S. Saroiu, Y. Ganjali, and A. Wolman, "Lockr: better privacy for social networks," in *CoNEXT'09*. ACM, 2009, pp. 169–180.