Unlinkability Support in a Decentralised, Multiple-identity Social Network

Simon Thiel[1], Fabian Hermann[1], Marcel Heupel[2], Mohamed Bourimi[2]

[1]Fraunhofer IAO
Nobelstraße 12
70569 Stuttgart, Germany
surname.name@iao.fraunhofer.de

[2]Universität Siegen
Hölderlinstr. 3
57067 Siegen, Germany
name@wiwi.uni-siegen.de

Abstract: Providing support for unlinkability in a decentralized, multiple-identity social network is a complex task, which requires concepts and solutions on the technical as well as on the user-interface level. Reflecting these diverse levels of an application, this paper presents three scenarios to impede the linkability of multiple identities in decentralized social networking. Solutions cover a communication infrastructure which allows referencing to multiple identities; analysis of user content and sharing history to present linkability warnings; and user interface means allow for a privacy-ensuring management of partial identities. The di.me userware research prototype of the EU FP7 funded digital.me (di.me) is introduced to show the integration of the solutions accordingly.

Introduction

Social networking and personal information management are closely connected fields for end-user applications: personal content, and information describing the person, is organised within diverse applications and services, and shared or disclosed when communicating and collaborating with others. However, in the Social Web, privacy and data protection are an issue often debated and criticised by data protection commissioners and citizens. Several technological trends and initiatives aim to empower users to have more control over personal data, e.g. emerging implementations of *decentralised social networks* [YL09]. Diverse initiatives base on the approach to provide personal servers as collection centres for the user's data (e.g. FreedomBox[1], Friendica[2], Cunity[3], VRM[4]).

[1] http://freedomboxfoundation.org
[2] http://friendica.com/
[3] http://www.cunity.net/
[4] http://cyber.law.harvard.edu/projectvrm/Main_Page

The di.me platform for decentralised social networking

The European funded project digital.me[5] (di.me) adopts the approach of decentralisation for social networking.

The research prototype "di.me userware", developed as the major outcome of the project and published as open source,[6] provides decentralised social networking and privacy-enhanced social functionalities based on a semantic model as its key features. A running prototype environment is currently hosted by the di.me consortium, and tested within the evaluation phase of the project.[7]

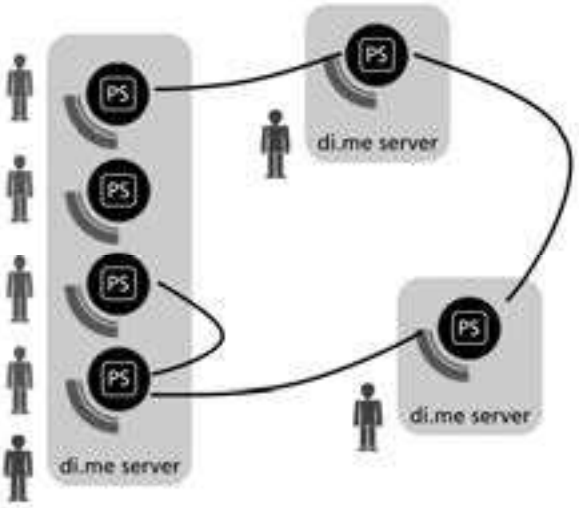

Figure 1: di.me userware network with di.me servers
hosting 1 or up to N Personal Services (PSs) for users

The di.me userware is subdivided into three packages: (1) the di.me server, containing the main functionality, (2) the di.me client, providing user interfaces (UI) for accessing the di.me server and (3) the di.me cloud, incorporating the necessary infrastructure required for setting up a decentralized network of di.me servers.

The decentralized approach is realized as a network of di.me server nodes communicating via HTTPS REST interface (REST-API). Each server is able to transparently host *Personal Services (PS)* for a number of users (Figure 1). The di.me PS represents the virtual personal node of a user.

This flexible solution allows for different hosting setups: a user may either use a single PS on a self-hosted server or apply for a user account as a tenant on a server provided by a trusted third party.

[5] http://www.dime-project.eu
[6] https://github.com/dime-project/meta
[7] For the evaluation environment see http://www.dime-project.eu

On the application level, the PS provides networking functionality. Messaging, document and profile sharing is supported between di.me PSs and also by use of external communication channels, e.g. by sending messages to twitter. Personal information from other sources (e.g. LinkedIn, Facebook, etc.) can be integrated by service adapters and semantic data representation standards. Based on this, the di.me userware provides pro-active functionalities [SC12] to the user, such as trust warnings, merge recommendations and situation detection. The case of recommendations to avoid content-based linkability is presented below in this paper.

At an architectural level, the di.me userware has been built upon a multi-layered approach native to dynamic web applications, providing a decoupled component schema that benefits future scalability requirements. For secure information management, the reference implementation provides a rich subset of semantic models, in compound with access control, processing components (such as the Sesame framework), and higher-level access APIs.

Like for PS-to-PS communication, also the UI clients connect to the PS accessing the di.me server's REST-API. The API establishes a generic way to access the user's PS. This supports clients with different functionality scope and running on various operating systems. Within the scope of the digital.me project a web-client and a client for Android mobile phones have been developed and are included in the OS publication.

Multiple partial identities

Many (centralised and decentralised) social networks offer advanced privacy settings, allowing for the filtering of information shown to contacts. With these settings – often at the level of the UI – the users can adjust which parts of their identity information are shown to others. While this can be considered as support of partial information sets linked to a root identity, di.me supports partial identities [PH10] which are potentially fully distinct information sets that can be shown to communication partners. In the process of sharing information, a partial identity can be used to control the specific set of personal data to be shared with individual contacts or groups. Such identities might become linkable to each other or to the person in real-life and could therefore possibly threaten users' privacy by revealing more information than intended. Consequently, the provision of *unlinkability* support is an essential feature for the di.me userware. Following the definition of [PH10], we define unlinkability of two items as the inability of an attacker to decide if they are related or not. In the case of di.me, such items are e.g. profiles which are indirectly representing an identity of a di.me user, and their attributes, in particular unique attributes like e.g. email address.

Unlinkability support in di.me

The following sections describe the unlinkability support in di.me, based on multiple identities. We focus on the following three different scenarios where identity linkability may be impeded with different technical means:

(1) Scenario 1: Linking (partial) identities to each other or to the person's root identity[8] by analysing the technical communication protocol (e.g. IP address discloses a physical location). This reduces the anonymity possibly leading to the revelation of the "real-life identity".
(2) Scenario 2: Linking a digital (partial) identity to the person's root identity because of disclosed information by the person him-/herself or by others[9] (e.g. the user's real-life or email address, his/her current geo-location, etc.).
(3) Scenario 3: Linking different (partial) identities to each other, because the same information is contained or shared via those identities (e.g. the same document shared under two pseudonyms).

The next section describes the requirements background of di.me with focus on the threats analysis. Based on this, the following sections detail di.me concepts and solutions for the scenarios of unintended linking of identities. Di.me combines solutions on the network and application communication level, as well as user recommendations and UI means to support the user.

Requirements background and threats analysis

A further requirements-driven analysis mainly based on the comparison of existing social networking led to the identification of five high-level requirements categories (cf. [TB12]) candidate to demonstrate innovation: (Category 1; **C1**) Integrated Personal Information Management, (**C2**) Secure, Privacy-respecting Sharing of Personal Information, (**C3**) Intelligent User Support with Context Sensitive Recommendations and Trust Advisory, (**C4**) Transparent Multi-Platform UI, and (**C5**) Integration of Existing Services. In the focus of this paper are the categories **C2** and **C3** by considering interdependencies to the other categories. The di.me open trust, privacy, and security infrastructure fulfill the major security goals, namely, *Confidentiality*, *Integrity*, and *Availability* also acronymised as the CIA Security Triangle. According to Santen in [S06], from the three major goals, confidentiality "*is one of the most practically difficult to achieve whereas integrity and availability can be achieved by means of standard software engineering techniques.*" Confidentiality goes beyond protecting the content of messages to protecting communication relationships in general (e.g. by means of anonymisation, i.e. pseudonimity), as this could reveal a lot about involved parties in such communications, i.e. the identities of senders and receivers allowing for different forms and degrees of linkability. Further, Santen also states that the interpretation of confidentiality (and the other protection goals) depends on application circumstances and scenarios to be supported: They can be classified by defining the attacker model within a threats analysis. Such model can be defined by answering the question "who may gain information and who must not". Thereby it is important for the stakeholders (i.e. all involved parties) to have some idea of who might assume the role of an attacker and

[8] For simplicity we use the concept of a root identity reflecting unique attributes of the respective person's real-life. In di.me the root identity is defined by the superset of the established partial identities.
[9] For instance a contact disclosing in a status update where s/he is and with whom by using real-life attributes („I m with Bob and Marry in Rome"). Such information could lead to linking these real-life attributes to used pseudonyms, e.g., if represented on a map functionality offered by the social network by using pseudonyms representing partial identities of Bob and Marry and their contact

what kind of behaviour (malicious or not) to expect from an attacker by performing a threats analysis. In this respect, correlations among protection goals and stakeholders (e.g. end-users, provider(s), and legislative)[10] could lead to conflicts, which is a classical multilateral security concern [R00]. As di.me supports multiple-identities it is crucial to integrate unlinkability support within. Linkability as non-functional requirements (NFRs) may conflict with other competing NFRs such as providing collaboration awareness[11] (in the UI) or negatively affecting user experience (in terms of performance penalties by using anonymity networks). The security requirements and threats analysis with respect to tasks of **C2** and **C3** was carried out by following the AFFINE methodology [BB10]. This enforces the early consideration of multilateral security requirements along with other (N)FRs by involving all stakeholders, negotiating, and aligning their potentially conflicting interests in the design[12] and development process.[13]

The requirements for our scenarios 1, 2, and 3 are addressed with a set of approaches solving specific linkability problems and implemented within di.me's open trust, privacy, and security (TPS) infrastructure. In the following, these solutions are summarized by showing how the TPS infrastructure enables di.me users to securely use and share personal data by considering respective threats analysis.

Avoiding linkability on a network and application communication level (scenario 1)

Derived from the first scenario of linking information items or persons, an important technical requirement is that the IP of the di.me server hosting the PS of a user must not be revealed as part of the communication protocol. Otherwise, the number of potential owners of an identity can be drastically reduced by the potentially low number of users hosted on a single di.me server.

Although the application of a PS is bound to a specific di.me server, the role of the server is transparent for the communication between two di.me PSs. Therefore, the information about the physical location of a PS is not required on this level of communication (e.g. when connecting for exchange of information, for sending of liveposts or for sharing). However, to hide a di.me server's location in the communication flow, when accessing a foreign PS, is a non-trivial task. Based on three main iterations, a solution for this has been developed for the di.me system (see also [BH12], [FH12], and [SB13] respectively):

[10] This is also the case in di.me since different parties from academia, research, and industrial fields are involved

[11] Social, group, and workspace awareness answering „who" is collaborating with „whom", „where", and „when"

[12] The solution's design process compromises consideration of an attacker model and threat analysis

[13] Santen begun the motivation of his work by citing from Viega and McGraw 2001 who stated that "*Bolting security onto an existing system is simply a bad idea. Security is not a feature you can add to a system at any time*". He further argues that "*the discipline of "Security Engineering" is far from mature today, and that, in practice, it still is not an integral part of the engineering processes for IT systems and software is based on the fact that security awareness results from reports on attacks – and not from the latest security feature that would make an application even more secure than it already was before*"

- Addressing of identities by use of a unique ID: at the level of the platform design as an internal reference to a specific identity was introduced, the Service-Account-ID (SAID).
- Hidden resolving of the SAID within a di.me proxy layer
- Concealing network communication flow by using the Tor[14] network

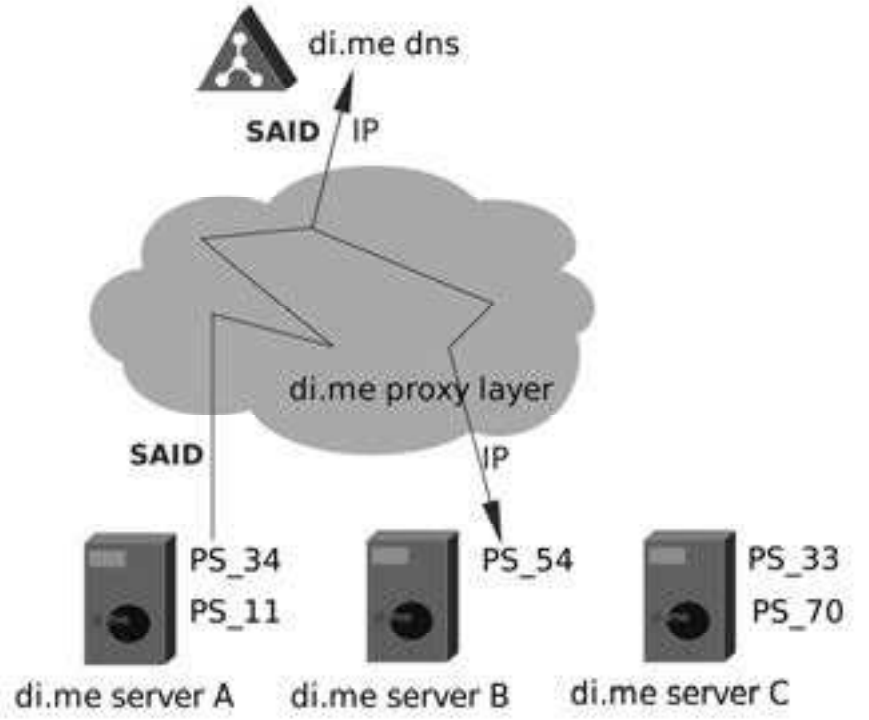

Figure 2: di.me proxy layer hides IP address of the PS providing a resource.

As alternative to an initial realisation relying on the Tor network, in which the attacker model does not trust any party, in the di.me environment [BH12], a di.me proxy layer, acting at the same time as an anonymity network has been designed (Figure 2). This flexible solution enables di.me to support end-users as well as business anonymity needs for (decentralised) social networking scenarios. It allows tailoring the anonymity degree according to needed privacy degree in the respective scenarios as a means for meeting multilateral security. A parallel usage of the Tor is still possible.

In order to actually contact another person's PS the corresponding SAID needs to be resolved. Therefore, a specific di.me DNS has been developed, allowing the translation the unique identifier to a network address, which can be either an IP, a forwarding proxy or a Tor-Onion address. As described in [FH12], it is also possible to be reachable over

[14] https://www.torproject.org

different channels at the same time. Therefore, it is possible to use the direct IP address for communication with close friends, while an anonymous/pseudonymous identity uses, for example, the Tor network.

A second important requirement is that IDs used internally as references to shared items must not be re-used when sharing via different identities. Otherwise, a receiver that is receiving shared items from two apparently independent senders is able to link these identities by comparing the IDs, even when the shared content is not unique. To resolve this, a concept of masquerading of shared internal IDs was developed: IDs used internally are mapped to anonymised IDs used for sharing as a single identity only. For further communication between PSs and the used name services and proxies, the anonymous credential system (anonymity at application layer) allows for balancing some linkability risks and threats as described in [PB13]. At the technical level, we leveraged *idemix* [CL00] along with OAuth for showing how other users could be retrieved within the di.me environment from a user's PS. The described technical solution is agnostic from the underlying social networking protocol used for enforcing authorisation in the respective server resources (e.g. OAuth). Special focus was also put on the support of mobile devices for future identity management scenarios since those devices are still have restricted anonymity support at the network as well as the application level.

User recommendations to avoid content-based linkability (scenarios 2 and 3)

Even though di.me is a decentralized solution unwanted information disclosure and linkability issues cannot be not completely avoided (accidental or intentional).[15] Santen [S06] points out that also user errors, in particular disclosing linkable information, may be used by attackers. The approach followed within di.me consists of (1) increasing the awareness of users by warning them during risky information sharing activities; and (2) engineering the system to securely process data and to help detect potential threats, e.g. when aggregating contact's information.

To sustain unlinkability of multiple identities of a single user, an approach is to control the potential linkability of partial identities. Therefore, the di.me userware analyses profiles and published information in order to find identifiability sets (a set of attributes identifying an individual user within a set of other users [PH10][Br05][Cl94]) and provides recommendations to the user based on that. This technique can also be applied even before information is shared in order to warn the user about potential privacy risks (e.g. when two contacts receiving different information might be the same person). In both cases, the di.me userware utilises techniques like semantic matching and semantic lifting to analyse textual information (see [CS12], [BR12] and [HB13]). This is used on the one hand to detect similarities in profiles of contacts and trigger a merge recommendation. On the other hand, profiles are compared and the user is warned accordingly, when linkability risks occur.

[15] By the users themselves or by others, e.g. by third parties (s. above example or someone disclosing information about his/her contacts)

Further, semantic analysis is applied on text and status messages written by the user to detect privacy threats because of shared information. For this, messages are decomposed into named entities and matched to identify persons, places, activities, etc. This text-analysis can be used to present privacy-enhancing recommendations to users. A prototype implementation shows warnings to the user that potentially sensitive information about third persons is being shared if contact names together with place or activity information is contained in a written text.

User-awareness on partial identities in the UI (scenario 3)

Many studies (cf. [CG06] and [KF10]) show that the UI plays a central role in handling privacy preferences and interpreting privacy notifications in threat situations like intentional or accidental information disclosure. Within a system offering multiple partial identities, the UI is a central mean to support the user's understanding of the segregation of identities [AW13], their distribution in the social network, and for avoiding undesired linkability (scenario 3). The di.me UI shall foster the user's awareness of multiple identities, the privacy preferences, and sharing history, and offer means to manage and control them. For representing identities within a user's PS, a UI object "profile card" has been chosen [HS13]. By selecting a profile card, e.g. for sharing an information item via it, the user selects the identity information shown to the recipient, *and* the SAID representing the identity on the network level. The decision to combine the selection of the SAID with the profile card was taken in order to reduce the UI complexity (for a discussion of usability and test results see [HS13]).

In the di.me approach the system supports the user in selecting the appropriate profile card (and this way implicitly the identity) to be used for sharing or communicating. Heuristics for that cover several rules, like suggesting profile cards already known to a recipient, profile cards already used for sharing a particular information item, or – based on di.me's recognition of contexts [SC12] – profile cards related to a current situation or sharing context. However, complex cases cannot easily be covered by heuristics. E.g., when multiple recipients are selected, no single profile card may be identified as sharing identity.

For such cases, di.me provides linkability warnings based on the sharing history: The system shows warnings that a selected profile card was never shared to a recipient before, or that a profile card (and other information item) will be shared outside the usual groups.

Summary and Outlook

The requirements for supporting unlinkability scenarios in a decentralised, multiple-identity social network comprise efforts on the technical level, the level of the UI and pro-active support e.g. in terms of recommendations and warnings. For three scenarios, di.me implements approaches to impede the linkability of multiple identities: A proxy layer as communication infrastructure is combined with SAIDs which allows reference

to identities independent from the IP address of the corresponding PSs. As result of this, analysing the technical communication protocol to link shared information to a root identity is inhibited. On the level of user content, di.me analyses the messages and profile information to find identifiability sets. Based on this, warnings about potentially critical content are presented. Warnings are triggered when information is being shared in order to make the user aware of potentially unintended linkability of partial identities and the root identity. Finally, the UI is designed to avoid privacy and linkability risks: Based on the UI object "profile cards", representing the user's partial identities, the user shall be enabled to control, and manage partial identities. To further support the user avoiding unintended disclosure of identities, warnings based on the sharing history are provided.

For the di.me userware as decentralised social network, these solutions form an integrated approach to avoid linkability of the offered multiple identities. To evaluate the approach, a prototype has been developed and implemented within a testing environment. The current version comprises of support for SAID resolving, sharing and communication using profile cards, and warnings based on sharing history and context. Further solutions, e.g. additional context-based heuristics for user recommendations, shall be incorporated and tested within the main demonstrator and the open source project. Recently started evaluation activities offer the prototype to a larger group of test-users and aim at gathering usability results as well as general feedback to the acceptance of the presented solutions for privacy-ensuring social networking. While preliminary results on the general concepts appear promising, further results on linkability advisory and other specific features are pending.

Acknowledgement

The work carried out in order to write this paper was supported by the Seventh Framework Program of the European Union, (FP7/ 2007- 2013), in the digital.me project under grant agreement no. 257787.

References

[AW13] Angulo, J., Wästlund, E.: Identity Management through "Profiles": Prototyping an Online Information Segregation Service. In Lecture Notes in Computer Science. Human-Computer Interaction. Users and Contexts of Use (pp. 10–19). Berlin Heidelberg: Springer (2013).

[Br05] Brands, S.: A primer on user identification. The 15th Annual Conference on Computers, Freedom and Privacy, Keeping an Eye on the Panopticon: Workshop on Vanishing Anonymity, Seattle. 2005.

[BB10] Bourimi, M., Barth, T., Haake, J., Ueberschär, B., Kesdogan, D.: AFFINE for enforcing earlier consideration of NFRs and human factors when building socio-technical systems following agile methodologies, in Human-Centred Software Engineering, ser. Lecture Notes in Computer Science, R. Bernhaupt, P. Forbrig, J. Gulliksen, M. Larusdottir, Eds. Springer-Verlag, 2010, vol. 6409, pp. 182–189.

[BH12] Bourimi, B., Heupel, M., Westermann, B., Kesdogan, D., Planaguma, M., Gimenez, R., Karatas, R., Schwarte, P.: Towards Transparent Anonymity for User-controlled Servers Supporting Collaborative Scenarios. In Ninth International Conference on Information Technology: New Generations (ITNG), pages 102–108, April 2012.

[BR12] Bourimi, M., Rivera, I., Scerri, S., Heupel, M., Cortis, K., Thiel, S.; Integrating multi-source user data to enhance privacy in social interaction. In Proceedings of the 13th International Conference on Interaccion Persona-Ordenador, INTERACCION '12, pages 51:1–51:7, New York, NY, USA, 2012.

[CL00] Camenisch J., Lysyanskaya, A.: An efficient system for non- transferable anonymous credentials with optional anonymity revocation, in Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology, ser. EUROCRYPT '01. London, UK, UK: Springer-Verlag, 2001, pp. 93–118.

[Cl94] Clarke, R.: Human Identification in Information Systems: Management Challenges and Public Policy Issues, Information Technology & People, Vol. 7 Iss: 4, pp.6 – 37. 1994.

[CS12] Cortis, K., Scerri, S., Rivera, I., Handschuh, S.: Discovering semantic equivalence of people behind online pro_les. In Proceedings of the 5th International Workshop on Resource Discovery (RED 2012), 2012.

[CG06] Cranor, L., Garfinkel, S.: Security and Usability. O'Reilly Media, Inc. (2005)

[FH12] Fischer, L., Heupel, M., Bourimi, M., Kesdogan, D., Gimenez, R.: Enhancing Privacy in Collaborative Scenarios Utilising a Flexible Proxy Layer. In International Confernce on Future Generation Communication (FGCT). IEEE Computer Society, 2012.

[HB13] Heupel, M., Bourimi, M., Scerri, S., and Kesdogan, D.: Privacy-preserving concepts for supporting recommendations in decentralized OSNs. In Proceedings of the 4th international workshop on Modeling Social Media, MSM '13, New York, NY, USA, 2013.

[HS13] Hermann, F., Schuller, A., Thiel, S., Knecht, C., Scerri, S.: The di.me User Interface: Concepts for Sharing Personal Information via Multiple Identities in a Decentralized Social Network. In Lecture Notes in Computer Science. Human-Computer Interaction. Users and Contexts of Use (pp. 29–38). Berlin Heidelberg: Springer. (2013)

[KF00] Krontiris, I. Freiling, F.: Integrating people-centric sensing with social networks: A privacy research agenda. In Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on, pages 620 –623, 29 2010-april 2 2010.

[PH10] Pfitzmann, A. Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version v0.34). 2010. Retrieved from http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (Last access: July 2013).

[R00] Rannenberg, R.: Multilateral security a concept and examples for balanced security, in Proceedings of the 2000 workshop on New security paradigms, ser. NSPW '00. New York, NY, USA: ACM, 2000, pp. 151–162.

[S06] Santen, T.: Security Engineering: Requirements Analysis, Specification, and Implementation. Habilitation, Fakultät Elektrotechnik und Informatik, Technische Universität Berlin (2006).

[TB12] Thiel, S., Bourimi, M., Gimenez, R., Scerri, S., Schuller, A., Valla, M., Wrobel, S., Fra, C., Hermann, F.: A requirements-driven approach towards decentralized social networks. In Future Information Technology, Application, and Service, volume 164 of Lecture Notes in Electrical Engineering, pages 709–718. Springer-Verlag, 2012.

[SB13] Schwarte, P., Bourimi, M., Heupel, M., Kesdogan, D., Gimenez, R., Wrobel, S., Thiel, S.: Multilaterally secure communication anonymity in decentralized social networking. To appear in IEEE Xplore as part of the proceeding of: 10th International Conference on Information Technology: New Generations (ITNG 2013).

[SC12] Scerri, S., Cortis, K., Rivera, I., Hermann, F., Bourimi, M.: di.me: Context-Aware, Privacy-Sensitive Management of the Integrated Personal Information Sphere. In 9th Extended Semantic Web Conference (ESWC2012). 2012. Retrieved from http://data.semanticweb.org/conference/eswc/2012/paper/project-networking/372/html (Last access: July 2013).

[YL09] Yeung, C., Liccardi, I., Lu, K., Seneviratne, O., Berners-Lee, T.: Decentralization: The Future of Online Social Networking. W3C Workshop on the Future of Social Networking. 2009. Available at http://www.w3.org/2008/09/msnws/papers /decentralization.pdf (Last access: July 2013).