Journal of Universal Computer Science, vol. 19, no. 7 (2013), 912-931
submitted: 31/8/12, accepted: 31/1/13, appeared: 1/4/13 © J.UCS

PETs at CSCL Service: Underutilised Potentials for Privacy Enhancing Distance Education

Mohamed Bourimi, Dogan Kesdogan, Marcel Heupel
(Chair for IT Security, Privacy, and Trust
University of Siegen, Germany
{bourimi, kesdogan, heupel}@wiwi.uni-siegen.de)

Dhiah el Diehn I. Abou-Tair
(School of Informatics and Computing
German Jordanian University, Amman, Jordan
dhiah.aboutair@gju.edu.jo)

Niki Lambropoulos
(Wire Communications Laboratory, Electrical and Computer Engineering Dept.
University of Patras, Patras, Greece
nikilambropoulos@gmail.com)

Abstract: Computer Supported Collaborative Learning (CSCL) support is currently widely accepted to provide reliable and valid formal and informal educational practices as proven to benefit students in onsite as well as distant educational settings. However, some results from case studies indicate that privacy problems could negatively affect CSCL implementation in educational settings. Privacy Enhancing Technologies research (PETs) and the development of multilaterally secure systems are still limited research topics within CSCL due to diverse reasons. Based on deep related literature analysis and previous research results conducted by the authors in building CSCL systems, three main categories were identified for such reasons that have an impact in PETs and multilateral security research: lack of awareness of such PETs' existence; lack of knowledge on ways to efficiently integrate them in CSCL systems and settings; and reluctance to consider their multilaterally secure implementation by CSCL participations due to conflict of interests (e.g. explicit students monitoring requirements, high integration costs, etc.). In this paper, these categories are addressed and the PETs potential is discussed for overcoming the associated emerging drawbacks focused on the distance education CSCL settings in particular. The result of our research is an integrated framework considering multilateral security requirements. Furthermore, proof of concept is provided; enhanced privacy in such settings is applied by demonstrating the fulfilment of selected improvements areas (i.e. mainly network, application anonymity, and process support for resolving potential multilateral security conflicts) in an existing collaborative distance education system.

Keywords: Privacy Enhancing Technologies, Multilateral Security, CSCL/CSCW, Distance Education, Social Settings, Network Anonymity, Anonymous Credential Systems
Categories: H.4.1, K.3.1, K.6.m, K.8.m

1 Introduction

Nowadays, a major trend in our current information technology age is to use diverse IT tools in many important sectors of our life activities such as business, health care,

education, entertainment, etc. Thereby we do not act only as an information font but also as a social outlet mainly by using the Internet as the global communication infrastructure. The modality of Internet based applications and tools evolved from tools supporting single-user usage to those that support multi-user usage by means of collaborative applications and systems. For instance, various universities[1], educational institutions and large organisations are using learning platforms in their learning and further education programs. Even more important are such platforms for universities specialised on education in form of distance and distributed learning. Nearly 700 studies indicate that collaboration in the educational sector leads to higher achievement, greater productivity and social competence, more caring and committed relationships, and self-confidence for students [Woolf, 2007]. Thus, CSCL support is being integrated in various platforms and virtual environments. For example, in a recent research study [Lambropoulos et al, 2012], CSCL social awareness and critical thinking levels tools were integrated within the open source learning management platform Moodle with positive results for all eLearning participants.

Since users are often interested in the collaborative construction of information and knowledge sharing, they are willing or sometimes forced, to disclose personal information in different life spheres and online communities in order to socially interact with each other. However, notable privacy risks of disclosing personal data in today's digital world exist especially in collaborative scenarios. This topic was broadly discussed in society and politics[2]: Both, the single users' disclosure of data on the Web for communication and social interaction, and the profiling and data gathering by economical players causes undesired consequences. This is mainly a result of the lack of control, as one's disclosed data to external parties is typically no longer under the users' control [Fraunhofer Institut für Sichere Informationstechnologie, 2008; Hildebrandt, 2008]. However, the broad diffusion of provider based data in products, markets and society also fosters inconsiderate and risky use of personal data, e.g. by younger users [The National Campaign, 2008]. In general, end users need to be supported to avoid data risks to which they are exposed when taking part in collaborative scenarios in the digital social world. This is mostly done by providing a set of mechanisms Privacy Enhancing Technologies (PETs) [Fischer-Huebner, 2001] by covering the (multilateral) security and privacy needs of the target scenarios by respecting legal policies for data rights. For instance, anonymous and ephemeral communication between peers and services has the highest potential to negatively balance the advantages of disclosing personal data (e.g. for service personalisation) and the risks of the providers user profiling. Therefore, anonymisation at different levels (i.e. network layer level and application level) to hinder linkability and observability are core concepts to be followed.

In this article, we argue that PETs and realisation of multilaterally secure solutions remain underutilized in CSCL as well as other areas due to different reasons, which could negatively affect CSCL implementation in educational settings. Three of those reasons are ignorance of such PETs (i), lack of knowledge in

[1] Coursera Hits 1 Million Students, With Udacity Close Behind: http://chronicle.com/blogs/wiredcampus/coursera-hits-1-million-students-with-udacity-close-behind/38801

[2] For example, the interested reader is referred to the proceeding of the International Conference of Data Protection and Privacy Commissioners, http://privacyconference2012.org

integrating them in CSCL settings (ii), and existing conflicts of interests of involved parties (iii). The article introduces thoroughly researched and established PETs that can be used to enhance the privacy and security in CSCL settings primarily for distance education in order to address the gap emerging from (iii). The main focus is on anonymisation techniques that facilitate communication unobservability, (identity) unlinkability along with the integration of classical security mechanisms such as access control. With respect to (ii) and (iii), the latest technology is explored and management outcomes and adoption (e.g., protocols and tools for anonymous communication, multilateral security methodologies) from developed approaches in projects with similar privacy respecting collaboration/cooperation needs. Potential realisation is then presented for reaching enhanced privacy in such settings by discussing the fulfilment of identified needs in the form of an exemplary integration into an existing collaborative distance education system. The result of our research is an integrated framework addressing all these reasons within a single methodology in an agile way (i-iii).

The remainder of the paper is structured as follows. Section 2 analyses the problem along with derived requirements; in section 3 the proposed approach is presented and applied in section 4. The final section refers to conclusions.

2 Problem and Requirements Analysis

The following problem and requirements analysis is the continuation of authors' work described in [Bourimi et al., 2009b]. There, the need for tailoring privacy is addressed in CSCL and CSCW settings in general. The summary of that work is presented first and further needs that were collected over the last five years and addressed in various other publications are added (mainly [Bourimi et al., 2009a; Bourimi et al., 2010a] as well as various related publications[3] published in the context of the digital.me project[4] owning a similar collaborative security and privacy needs).

2.1 Background information

The work described in Bourimi et al. [Bourimi et al., 2009b] addressed privacy needs identified by using the CURE platform [Haake et al., 2004a] for typical CSCL and CSCW scenarios. The CURE (Collaborative Universal Remote Education) platform was developed to support different learning scenarios at the German Distance Learning University. The requirements analysis was based on the analysis of intended scenarios within the university by involving users from various disciplines like mathematics, electrical engineering, computer sciences and psychology. Since fall of 2004, CURE is an integral part of the university's virtual learning space and has currently more than 3000 registered users at this time.

The consideration of privacy in CURE was considered at different levels (e.g. collection of anonymised log data for evaluation, usage of pseudonyms for login, etc.). At the technical level, the used databases for performing authentication were separated according to the German privacy laws and followed by privacy supervisors.

[3] http://www.wiwi.uni-siegen.de/itsec/projekte/dime/index.html.en
[4] http://www.dime-project.eu

Where possible, the usage policy enforced enabling some features (such as user list or activity indicators) since collaborative/cooperative settings need some degree of user-information disclosure within the system in order to achieve the intended collaboration goals [Palen and Dourish, 2003]. However, since mostly no one reads usage policies [Gindin, 2009], the usage of some collaboration means in CURE (such as a persistent chat, some awareness functions like presence indicators at the level of the user interface, etc.) were not appreciated by some users. A result of such disagreement was stagnation in the usage of the system. [Tang et al., 1994] stated that users are often cautious about how the system handles their privacy and are afraid that their mistakes will affect their reputation. According to observations, many students restricted their interactions in the collaborative environments to the minimum or used in parallel their own collaboration tools, which are not under the control of the instructors.

In general, studies show that inhibition of users regarding privacy and trust concerns may negatively affect their interaction with and trust in the platform. Just to name a few: A very representative statement for similar concerns in the e-learning field can be found in [Borcea-pfitzmann et al., 2005]: *"The goal of security in e-learning is to protect authors e-learning content from copyright infringements, to protect teachers from students who may undermine their evaluation system by cheating, and to protect students from being too closely monitored by their teachers when using the software. Since these intertwined requirements are not met by existing systems, new approaches are needed."*. Another statement can be found in [Aïmeur et al., 2008] the authors state"*E-learning systems have made considerable progress within the last few years. Nonetheless, the issue of learner privacy has been practically ignored. Existing E-learning standards offer some provisions for privacy and the security of E-learning systems offers some privacy protection, but remains unsatisfactory on several levels."*

The proposed solution to solve privacy and trust problems in the CURE platform were to introduce a decentralized group-centric approach for tailoring collaboration according privacy needs. In contrast to the traditional centralized usage of collaboration environments, the proposed decentralized group-centric approach gave each group the whole responsibility of hosting the collaboration environment by using their own technical means. In general, supporting such approach where the user is hosting the learning environment for his/her trusted fellow students, ensures full user-control by building trusted groups. From security point of view, decentralization offers the most possible decision freedom for the end user at all levels (i.e. where and how to deploy and so on). Decentralized social networks promise more user control with respect to information disclosure. Server-centric approaches mostly imply that the server is the central point of information exchange, which allows building of fully-fledged user profiles of involved entities and may lead to many other linkability and security issues.

The implementation provided a prototype consisting of a collaborative platform and its ubiquitous pendant. The latter is installed, managed and hosted by the individual groups themselves using their own hardware. The prototype realises a star topology where the central node represents the main platform of the collaborative system (allowing sharing between group-focused environments) and the surrounding nodes represent the end-users' ubiquitous platforms (hosting the group-focused

environments). User groups are able to share their data with other groups or even other collaborative environments, by having complete control over their data. That approach is based on encouraging users trusting each other to work together without the pressure that all interaction traces can be monitored and evaluated. Information can only be shared with explicit consent.

2.2 Advanced Privacy Enhancing Technologies and CSCL

Whereas [Bourimi et al., 2009b] tried to satisfy privacy needs for collaboration on an architectural level (i.e. by means of decentralisation), the majority of well-known learning (management systems) and CSCL platforms follows a centralised architecture. Even though all those platforms use PETs for providing basic security functionality[5] they do not sufficiently address privacy protection goals, especially from the multilateral security point of view [Pötzsch et al., 2011]. The usage of advanced PETs remain underutilised, namely a variety of technologies that protect personal data by minimising or eliminating the collection of personal data and so on which can become much appreciated especially in collaborative settings [Liesbach et al., 2011]. The most currently available implementation of PETs in CSCL systems has either a server-centric architecture or a client-centric/user-centric architecture. Client centric approaches are not sufficient and suitable for collaborative environments since the exchange of information is the base of such environments. Server-centric approaches require a great amount of trust at the server [Agrawal et al., 2003].

With respect to privacy in Computer Supported Collaborative Work (CSCW) systems in general[6], one can mention the deep analysis of privacy-related literature for such collaborative environments considering different perspectives is given in [Boyle and Greenberg, 2005] and [Boyle et al., 2008]. Mostly, privacy problems result from supporting data sharing and provision of awareness[7] functionality. Group awareness [Gross et al., 2003, Gutwin, 1997] can help to reduce the number of possible conflicts by establishing a social protocol. However, apart from that provision of awareness conflicts with privacy according to Boyle and Greenberg in [Boyle and Greenberg, 2005] with respect to (1) privacy violations and (2) user disruption. Solving these issues by considering focus on collaboration support remains subject of contemporary research. In order to bypass such issues many research projects investigate benefits of PETs for collaboration in general such as the integrated EU project PRIME[8] ("Privacy and Identity Management for Europe"), its finished followers PICOS[9] and PrimeLife[10] ("Bringing sustainable privacy and identity management to future networks and services"), and the still running projects ABC4Trust[11] as well as di.me[12] ("Integrated

[5] Known as CIA triangle: Confidentiality of communication, Integrity of processed data, and its Availability.
[6] The reader may notice that CSCL is the implantation of CSCW results for the specific area of E-Learning
[7] Knowledge about various things as who is in the collaborative environment, what is s/he working on, and what s/he is doing and so on.
[8] http://www.prime-project.eu.org
[9] Privacy and Identity Management for Community Services, www.picos-project.eu
[10] http://primelife.ercim.eu
[11] "Attribute-based Credentials for Trust", https://abc4trust.eu
[12] www.dime-project.eu

digital.me Userware"). In general, the current state of consideration of PETs in CSCL is summarised based on authors' contribution in building CSCL systems and many of the previously cited projects[13] that:

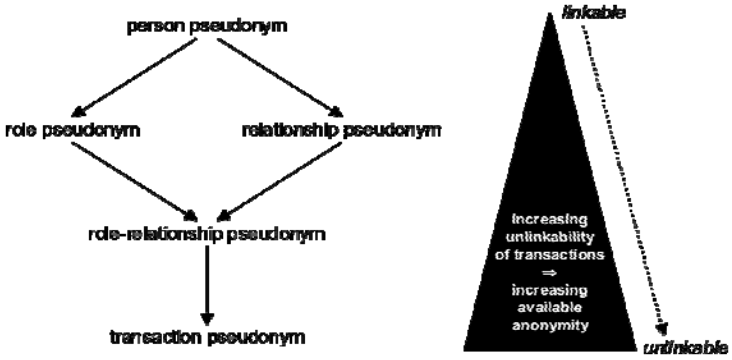

Figure 1: Pseudonymity and linkability degree [Pfitzmann, 1990]

1. Ignorance of advanced PETs: to solve privacy issues consists in using access control for restricting access to sensitive information. Another way consists of providing a possibility to refer to members without revealing their true identities in authentication routines, i.e. with pseudonyms closely linked to partial identities. However, most of people ignore the existence of the existence of anonymous credential systems that enhance the privacy for used credentials just by providing proofs that one is fulfilling the minimal requirements for authentication needed by the system (see Figure 1) **(C1)**.

2. Lack of knowledge in integrating them in (CSCW/CSCL) settings: For instance, recent research conducted by the authors is shown that even though anonymity solutions along with SSL certificates is used to hide location of platforms in collaborative settings, linkability problems could arise. This leads to re-identifying persons and allow for many crucial attacks (e.g., Denial of Service or man-in-the-middle attacks). Another example is even though data is spread over different databases (sometimes at the level of the same educational institution), it is still possible that one infers data and re-identify people as Sweeney showed in [Sweeney, 2002]. Last but not least, when considering the increasing usage of social networks and their integration in E-Learning systems one should know that some works allow for re-identifying people with just an error rate of 12% as shown in [Labitzke et al., 2011; Narayanan and Shmatikov, 2009] **(C2)**.

[13] www.dime-project.eu

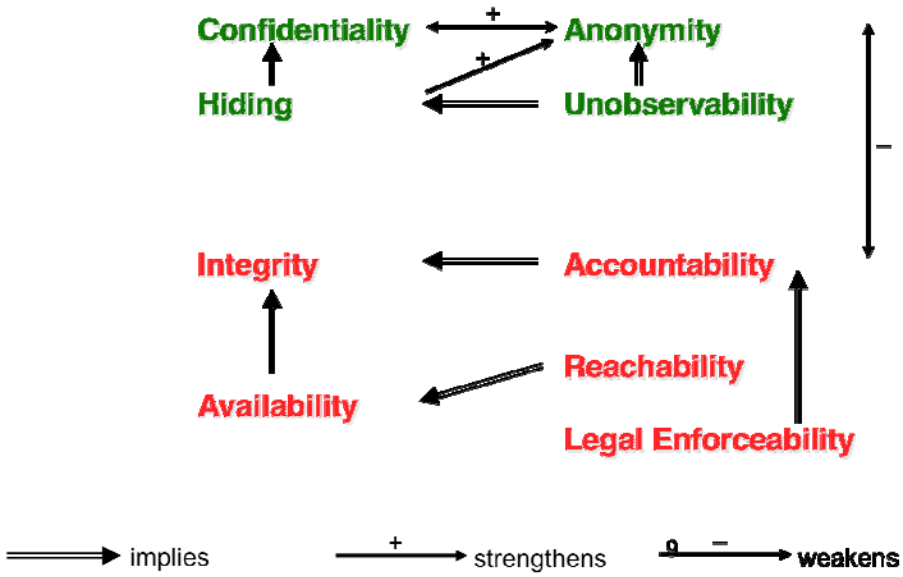

Figure 2: Correlation of protection goals [Wolf et. al., 2000]

3. The missing will to introduce them due to conflict of interests (e.g. explicit students' monitoring requirements, high integration costs, etc.): Including PETs for better end-users' privacy control is not a trivial task from the software engineering perspective. This is due mainly to the complex field of security and privacy as well as the correlations between protection goals (see Figure 2) in the same field as well as with other fields (e.g. usability of their usage). When considering that the final software system providing the wished CSCL support is the result of consideration of all functional as well as non-functional requirements (and not just privacy), one can imagine the challenge to align all non-functional requirements to be fulfilled, i.e. reflected in the domain model and user interface and so on. Poor design can results in privacy violations. Researchers in the CSCW, HCI and Security research communities generally assume that privacy issues arise due to the way systems are designed, implemented, and deployed **(C3)**.

3 Approach

Categories C1-C3 are addressed in this article like follows:

— C1 will be handled by introducing basic terminology, i.e., privacy and security requirements, as well as concepts of the security community and PETs

— C2 will be addressed by introducing the existing tools, protocols and solutions for fulfilling the main privacy and security requirements as building blocks
— C3 needs process support and consideration of advanced concepts like Multilateral Security reusing the building blocks in a scenario oriented manner.

3.1 Introduction of basic terminology (C1)

In the following section, the network and application anonymisation terminology is addressed, since both represent the two main subjects not familiar to non-security experts. Furthermore, both are used to show improvements in the exemplary CSCL system in the approach section.

3.1.1 Network anonymisation

Network-level anonymisation is concerned with providing confidentiality of traffic data. That is necessary, since even if the content of the traffic is encrypted, the event that a particular sender transmits a message to a particular receiver might be sensitive in itself. However, the sender and receiver of messages are visible in common network protocols as used in the Internet, thus requiring the additional usage of network anonymisation protocols to cover the sender and receivers identity. Research into network-level anonymity is widely regarded to have begun with the introduction of the Mix technique for untraceable electronic mail [Chaum, 1981]. In a Mix system, messages are not directly addressed to the receiver but are prepared to be relayed by so called Mix routers. Each message carries the addresses of the Mixes on the path to the receiver in an encrypted structure, with each relaying Mix on the path only seeing the address of the previous and decrypting the address of the next. To hide the relation between the messages arriving and those leaving a Mix, it mixes the output order of messages. That way, even an omnipresent passive attacker who can observe the act of sending and receiving messages at every Mix and senders and receivers, cannot link the sender and receiver of a message.

The most prominent anonymous communication systems are based on the Mix idea. Mixminion [Danezis et al., 2003] is a high latency system for anonymous mail transfer. Low latency systems target at enabling a broad range of multimedia traffic on the internet that are more time-critical than e-mails, therefore reducing the security of the Mix for the sake of increased network performance. These systems are represented by JAP [Berthold et al., 2001] and Tor [Dingledine et al., 2004] in practice. JAP and Tor do not provide mixing at the relay routers and can only provide protection against an attacker, who is not omnipresent. These approaches are popular in practice and widely used by governments and citizens in different countries.

3.1.2 Anonymous credential techniques

Network anonymisation combined with data anonymisation that operate on the application layer avoid the linking of information to single individuals, so that the source of that information is hard to identify. In some cases, this might not comply with the security requirement of the information receiver that might require proofs of the integrity of the source.

Anonymous credentials are application layer techniques that operate on top of network anonymity systems, making use of digital signature systems. By showing anonymous credentials, a user is able to only proof his integrity (e.g. an attribute that proves authorisation) without providing any further information about itself, that can be linked to the credentials shown in the past and in the future by the same user. In opposite to that, a normal credential certifies attributes for a particular user identity, and thus enables the linking of distinct data originating from that user.

The first anonymous credential system was introduced by [Chaum, 1985]. Succeeding approaches increased the performance and the usability of the credential system [Damgard, 1990], [Camenisch and Lysyanskaya, 2001]. Most notably *idemix* [Camenisch and Lysyanskaya, 2001] have been developed throughout several EU-Projects Prime and Prime Life. It is supported by IBM and is available for use. Microsoft provides by U-Prove [Brands and Paquin, 2010] an anonymous credential system that is less feature rich in comparison to *idemix*. This system is in some use cases more efficient than *idemix*.

3.1.3 Multilateral security

Motivation describes a subjective incentive that effects behaviour. Subjects as actors in processes introduce multiple, potentially conflicting motivations into processes, which induces different expectations about actions of subjects, especially with respect to multilateral security objectives. Thus, to reduce the amount of trust that has to be put into individual actors to behave in a specified way that might conflict with their motivations, multilateral objectives must be consolidated and potentially conflicting motivations and security objectives have to be recognised and made visible. [Sailer, 1998] defines "multilateral secure" by stating "A telecommunication service is called multilaterally secure, if and only if security goals of all parties that are affected by the service are taken into account in a balanced way".

Multilateral security [Rannenberg, 1994; Rannenberg, 2001] has been used to describe techniques and models that solve seemingly conflicting security objectives of multiple parties in a system. The term has been used in various fields, for example digital rights management where conflicts between the objective of the publisher to prevent unauthorised copies, and the need for privacy of the users are to be considered [Fischer and Eckert, 2008]. Since we are in this project talking about a way to measure and label the likeliness of conflicts (e.g., corruption, information leakage, etc.), the interesting point is when the extrinsic motivation (money received by an briber) is stronger than the intrinsic motivation to be honest. User privacy is also a concern in biometric access control systems, where this requirement conflicts with the effectivity of the biometric recognition [Bleumer, 2006; Westfeld, 1999].

This definition conflicts with the usage of the term in access control models, where multilateral security describes concepts to prevent lateral information flow

between compartments of an organisation, e.g. Chinese Wall Model or British Medical Association Model. Multilateral security there is orthogonal to Multilevel Security [Needham 2010].

3.2 The integrated framework considering multilateral security

Nowadays, different development methodologies with different degree of agility are followed when building sophisticated software systems. Even when applying these methods, non-functional requirements (NFRs) are often considered too late in the development process and tension that may arise between users' and developers' needs remains mostly neglected. Furthermore, there is a conceptual lack of guidance and support for efficiently fulfilling NFRs in terms of software architecture in general. The PET enabled CURE System (C2 & C3).

In general, efficient methods for requirement and software engineering are crucial in order to assure adequate systems and reduce development costs while fulfilling end-users' requirements in the presence of frequent changes. Multilateral security requires addressing [Rannenberg, 1994; Rannenberg, 2001]:

- Minimalistic End-User Trust (the trust of the end-user is minimal in the system to be developed/used)
- Individual Protection Goals
- Detection of Conflicts and Negotiation of Compromises
- Compromises' Accomplishment
- Interest protection of all stakeholders

From other projects (including the case study learning platform CURE, see next section), the following four requirements for development processes as well as implementation technology were derived considered as characteristic for collaborative systems subject to frequent changes [Bourimi et al., 2009a]:

- Systematically addressing NFRs (e.g. end-users' privacy concerns) early in the development process considering trade-offs with (N)FRs, Special focus is put on the alignment of the often contradictory multilateral security requirements listed above (High Level Requirement 1; HLR1: ANALYSIS)
- Addressing emerging changes in the business processes which can be efficiently tailored according to the steps or phases of the different existing development processes, practices and approaches (HLR2: AGILITY)
- Considering explicitly human factors (all stakeholders, namely, developers, end users, and parties with different protection goals etc.) in the method answering HLR1 and HLR2 (HLR3: HUMAN FACTOR)
- Supporting the method at the architectural and implementation level to assure meeting HLR1-HLR3 at minimal cost (HLR4: SYSTEM ARCHITECTURE).

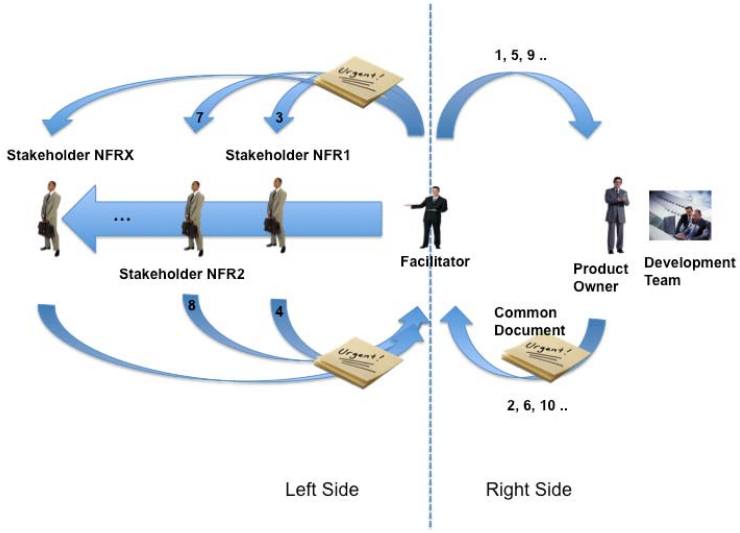

Figure 3: The Scrum based AFFINE method considering multilateral security

To satisfy HLR1-HLR4 we developed an integrated framework consisting of an iterative and agile method based on SCRUM[14] (HLR1-3) and its support through a generic software architecture (HLR4). The concrete approach involves in early design and development stages experts from all parties (see the left side in Figure 3). This enforces the consideration of multilateral security from the beginning. A further advantage is aligning the used technical terms among stakeholders including those addressed in C1. The right side is a typical Scrum loop. Further AFFINE details could be found in [Bourimi et al., 2010a] and its implementation for our case study in subsection 4.2.4.

4 Case Study

In this section, the main concepts and features of the proposed collaborative system and functionality are briefly discussed and extended, based on the work described in [Bourimi et al., 2009b]. After this, the ways the CURE system was retrofitted in order to support anonymity at network as well as application level is presented next.

4.1 The Collaborative System in a Nutshell

To model shared workspaces for groups CURE[15] uses the room metaphor. The virtual key metaphor is used to determine access rights and allowed interactions within a

[14] Schwaber, K.: Scrum overview (2009): http://codebetter.com/blogs/darrell.norton/pages/50339.aspx
[15] CURE: Collaborative Universal Remote Education http://www.fernuni-hagen.de/ks/projekte/85431.shtml

given room. Users who have keys to a certain room can form a group and so cooperate and work between each other. For instance the navigation tree view (Figure 4 A) is generated and shown for every user depending on his keys (e.g. users can see only rooms to which they have access to). Users who disposes about sufficient rights, i.e. for creating adjacent rooms, or passing on or copying their virtual keys, and editing the content, can therefore at any time adapt the collaborative environments according to their needs (also during the collaboration process).

Figure 4: User interface of the retrofitted CURE

For dynamic group formation without prior planning of the system administrator, end-users are able to form groups (1) by assignment, (2) by invitation, (3) with free enrolment, and (4) enrolment confirmed by the members of the respective groups [Haake et al., 2004b].

4.2 PET enhancements of CURE in detail

4.2.1 Enhancements by anonymous credential support (C2)

Management of access rights is in the middle of many collaboration forms such as group formation in different kinds of groupware. However, existing solutions often remain difficult for end-users. Evaluations of a first prototype identified the need for a sophisticated and practicable access control mechanism, to enhance the usability of privacy-respecting social interaction in collaboration such as transparently performing authorisation e.g. without any user intervention at the level of the user interface. The potential of using proof based credential systems like *idemix* is identified, which opens the possibility to anonymously proof possession of certain attributes. An exemplary use case is, e.g. access control to a discussion board for students.

Therefore all involved parties would receive special *idemix* credentials, enabling users to anonymously prove that they are e.g., a student or a professor without revealing anything else. This allows ensuring that only enrolled students gain access to the discussion board, while other parties (e.g., non-students, or professors) are prohibited. In [Bourimi et al., 2011], this exemplary is shown with means of a developed prototype mobile application for supporting collaborative scenarios for the upcoming EU project di.me[16].

4.2.2 Enhancements by network anonymity (C2)

The group-centric CURE allowed users to host on their own trusted nodes. By connecting to these nodes, it is important in some cases that the network location of the node as well as the location of clients connecting to that node remains hidden (e.g. to avoid DoS attacks or localisation issues). Such requirement emerged mainly based on the attacker model developed for the di.me project. This means, that the involved people in the trusted group might trust the hosting node but do not want to disclose their current location (which could be inferred based on their clients' network addresses). The other direction is that the provider of the node wants to hide its servers if someone of the group disclosed the location to untrusted people and so on.

Even though anonymity networks are being used, potential linkability issues are demonstrated, especially when those servers are used to support collaborative scenarios (e.g., communication and sharing with others). The requirement for anonymity at the network level should be supported in an efficient way also in terms of performance, described in [Bourimi et al., 2012; Fischer et al., 2012; Schwarte et al., 2013; Wrobel et al., 2013].

The proposed solution was based on binding the communication with all contacts of used identities to a Tor hidden service. In particular, a multi-process anonymity component is presented adding such hidden services at-runtime. With respect to Tor, an analysis of contemporary anonymity solutions led to the result that Tor is the most suitable anonymity network for collaborative systems and was oriented to the concrete purposes for di.me addressed above with respect to collaborative scenarios in general (inch potential P2P settings). However, the solution was also successfully integrated into CURE with less effort since the di.me result is made available in form of a pluggable component.

4.2.3 Further security related enhancements (C2)

Since the group-centric CURE allowed users to host on their own trusted nodes, new requirements emerged with respect to hosting. Cloud computing as a facility for user-controlled servers is a growing trend. Customer-driven application deployment in public clouds has to be secure and flexible by means of easing security configuration as well as by avoiding the vendor lock-in problem. The concrete requirements are related to (1) easing security configuration(s) in the deployment step, (2) automating the consideration of security best practices and adding/enabling anonymity components at-runtime (see4.2.1 and 4.2.2), and (3) by using a standard image for deployment of the environment in order to overcome the vendor lock-in problem. In

[16] http://www.dime-project.eu/

[Karatas et al., 2012] ESCAV-ISION is presented as a tool to meet these requirements. There, the need for enforcing the security of application deployment is identified with public cloud services at the IaaS layer. At the same time the vendor lock-in effect shall be avoided by using OVF for packaging applications. We empowered lay as well as expert users shall be supported in their outsourcing projects with a high-level view in order to increase the usability/ease of security configurations. Further, the ways balance was achieved between provider lock-in problems and the specific requirement of high-availability for different collaborative platforms is presented (which remains valid for CURE) by using LiveRebel since it does not affect the architecture or code of the respective architecture.

4.2.4 Process support for C3

As mentioned in [Bourimi et al., 2009a, Bourimi et al., 2010a], the CURE platform was developed at the FernUniversitaet in Hagen (FuH) by following an agile process called the Oregon Software Development Process (OSDP). Applying OSDP considered end-users feedback of the participating departments at the FuH. Representatives of students and instructors from various disciplines such as mathematics, electrical engineering, computer sciences and psychology were participating in the usage and evaluation of the prototypes resulting from each OSDP-iteration. Even though OSDP considers conceptually NFRs in form of a NFR backlog, their consideration was not earlier enough to overcome drawbacks in the construction phase. In the case of CURE, responding to end-users wishes related to NFRs (e.g. usability of the web interface, performance of the synchronous communication means and awareness provision in the shared workspaces) was interrupted in order to meet the delivery and integration deadlines and budget. CURE was extended in various sub-projects that were primarily concerned with improving NFRs which were classified as insufficiently covered by the developed system or tried to address new needs emerged through the usage of the system. For privacy related CURE extensions, meeting C3 in authors' research work AFFINE (Agile Framework For Integrating Non-functional requirements Engineering) was essential [Bourimi et al., 2010a] simultaneously addressing needs emerging from C3 at process and implementation level with:

- Conceptually enforcing the earlier consideration of all relevant NFRs (incl. multilateral security requirements) and possible trade-offs early in the development process
- Explicitly balancing end-users' with developers' needs when following agile development methodologies
- Supporting the development method at the architectural and construction level with a reference architecture focusing on implementation support for NFRs

AFFINE was successfully in earlier implementation in CURE and is being successfully applied in many projects at the authors' institute including the previous cited works above for enhanced support of C2. From these projects, the iAngle[17]

[17] http://www.uni-siegen.de/fb5/itsec/projekte/iangle/index.html

project and its following project iFishWatcher[18] are the most representative ones. Both projects reached product maturity even though developed in academic settings. The resulting application is available in Apples App Store and is being downloaded frequently, which indicates first acceptance signs. With respect to scientific research, one German national and ten international conferences and journal article publications resulted based on AFFINE. Thereby, more than eighteen researcher/experts and students were involved in the different iterations. Further representative projects are the Shopper Metrics project, and the funded projects EU FP7 digital.me[19] and BMBF RescuelT[20] (with respect to USIEGENs work packages). More especially, the re-use of results and their portability from one project to another (as partially did from di.me to PET enhanced CURE) is one of the outcomes of AFFINE.

5 Comparison to related work

As stated in section 2, the proposed three problem categories were identified based on the suggested contribution in contemporary EU research projects such as PRIME (http://www.fp7prime.eu/project), PICOS (http://www.picos-project.eu/) and di.me (http://www.dime-project.eu/). Based on this expertise, we argue that the identified needs and the way to solve them in this article is described, represent originality and relevance for research with respect to solving the stated problem, on how to improve the underutilisation of PETs for CSCL (and CSCW) in general on different levels.

In PRIME, the partner extended the eLearning platform BluES'n[21] to enable privacy enhancing identity management with the aim to protect personal user information (cf. [Borcea-pfitzmann et al., 2005], [Pötzsch et al., 2011], and [Liesebach et al., 2011]). The big drawbacks of BluES'n lay in the system performance and in the usability because of the influence of many transactions needed in order to apply privacy [Kellermann, 2008]. However, it was the first prototype for an E-Learning system supporting anonymous credential systems. BluES did not focus on CSCL but on basic E-Learning functionality and proposed approach described in [Bourimi et al., 2009b] provided an enhancement at the architectural level (by supporting decentralisation for trusted groups). Enabling CURE with anonymous credential functionality is described in the work [Bourimi et al., 2011] and highlighted in 4.2.1.

With respect to supporting network anonymity, authors' research work described in [Bourimi et al., 2012] and highlighted in 4.2.2 is to our best knowledge the first work addressing potential linkability in collaborative scenarios when using anonymity solutions like Tor. The proposed solution is implemented for the di.me project supporting decentralised networking and ported to the PET enhanced CURE even latter remains until now also a kind of prototype. The added value enhancement at process level was reached by using AFFINE [Bourimi et al., 2010b] for earlier consideration of (N)FRs by the realisation of socio-technical systems in general, and

[18] http://www.ifishwatcher.org/news.php
[19] http://dime-project.eu
[20] http://www.uni-siegen.de/fb5/itsec/forschung/projekte/rescueit/
[21] http://blues.inf.tu-dresden.de

solving potential multilateral security conflicts [Fischer et al, 2012; Karatas et al., 2013; Schwarte et al., 2013; Wrobel et al., 2013].

6 Conclusions

Computer Supported Collaborative Learning (CSCL) systems become nowadays more and more important and are used in different kinds of institutions and organisations. However, we argue based on our experiences and literature research that the consideration of advanced privacy enhancing technologies (PETs) is still underutilised in the Computer Supported Collaborative Work (CSCW) area in general, and the CSCL field in particular.

In this article, three main issue categories were identified and presented as a proposed approach to overcome their drawbacks, namely, an integrated framework considering multilateral security as well as privacy requirements. Basic terminology was first introduced for the security area mostly ignored or not well known by other communities. After this, added value improvements were concretely showed by addressing a series of works performed since 2009 (in the CSCL area), by improving the CURE platform supporting CSCL for distance learning (based on outcomes from other projects such as the EU FP7 di.me project). The platform was successively extended over the last year until today to support decentralisation, anonymous credential systems for advanced identity management, and network anonymity to avoid linkability in collaborative settings. Main improvements were not just at the technical level (i.e. cloud deployment by end-users) but also at process support level for aligning non-functional requirements when building socio-technical systems by explicitly considering multilateral security conflicts in that process support. The main target of this article, however, is to highlight the underutilisation of PETs potentials in the important field of CSCL since privacy could negatively affect its benefits. Since exemplary systems and many other related work conducted by the authors is still at the prototypic level, the adoption of PETs in CSCL remain in the hand of E-Learning and CSCL platforms providers mostly ignoring advanced PETs for now.

Acknowledgements

Parts of this work are supported by the digital.me EU FP7 project, funded by the EC (FP7/2007-2013) under grant agreement no. 257787. Thanks are also due to many members of the IT Security Management Group at the University of Siegen for the direct or indirect contribution to this article, namely, Lars Fischer, Vin Pham, Fatih Karatas, Philipp Schwarte and Jens Gulden.

References

[Agrawalet al., 2003] Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y. (2003). Implementing P3P using database technology. In ICDE, pages 595-606.

[Aïmeur et al., 2008] Esma Aïmeur, Hicham Hage and Flavien Serge Mani Onana (2008). Anonymous Credentials for Privacy-Preserving E-learning. In International MCETECH Conference on e-Technologies, pages 70-80. IEEE Computer Society.

[Berthold et al, 2001] Berthold, O., Federrath, H., and Kopsell, S. (2001). Web mixes: A system for anonymous and unobservable internet access. In Federrath, H., editor, Designing Privacy Enhancing Technologies, volume 2009 of Lecture Notes in Computer Science, pages 115-129. Springer Berlin / Heidelberg. 10.1007/3-540-44702-4.7.

[Bleumer, 2006] Bleumer, G. (2006). Biometric Authentication and Multilateral Security. In Multilateral Security in Communications, vol. 3, pp. 157-171.

[Borcea-pfitzmann et al., 2005] Borcea-pfitzmann, K., Liesebach, K., and Pfitzmann, A. (2005). Establishing a privacy-aware collaborative elearning environment. In in Proceedings of the EADTU Annual Conference 2005: Towards Lisbon 2010: Collaboration for Innovative Content in Lifelong Open and Flexible Learning.

[Bourimi et al., 2010a] Bourimi, M., Barth, T., Haake, J., Ueberschaer, B., and Kesdo-gan, D. (2010a). Affine for enforcing earlier consideration of nfrs and human factors when building socio-technical systems following agile methodologies. In Bernhaupt, R., Forbrig, P., Gulliksen, J., and Larusdottir, M., editors, Human-Centred Software Engineering, volume 6409 of Lecture Notes in Computer Science, pages 182-189. Springer Berlin / Heidelberg.

[Bourimi et al, 2010b] Bourimi, M., Barth, T., Haake, J. M., Ueberschar, B., and Kes-dogan, D. (2010b). Affine for enforcing earlier consideration of nfrs and human factors when building socio-technical systems following agile methodologies. In Proceedings of the 3rd Human-Centered Software Engineering Conference, Reykjavik, Iceland.

[Bourimi et al., 2009a] Bourimi, M., Barth, T., Ueberschaer, B., and Kesdogan, D. (2009a). Towards building user-centric privacy-respecting collaborative applications. In Tavangarian, D., Kirste, T., Timmermann, D., Lucke, U., and Versick, D., editors, Intelligent Interactive Assistance and Mobile Multimedia Computing, volume 53 of Communications in Computer and Information Science, pages 341-342. Springer Berlin Heidelberg.

[Bourimi et al., 2011] Bourimi, M., Heupel, M., Kesdogan, D., and Fielenbach, T. (2011). Enhancing Usability of Privacy-Respecting Authentication and Authorization in Mobile Social Settings by Using idemix (EU FP7 digital, me Project Technical .... researchgate.net.

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

[Bourimi et al, 2009b] Bourimi, M., Kiihnel, F., Haake, J., el Diehn I. Abou-Tair, D., and Kesdogan, D. (2009b). Tailoring collaboration according privacy needs in real-identity collaborative systems. In Carrico, L., Baloian, N., and Fonseca, B., editors, Groupware: Design, Implementation, and Use, volume 5784 of Lecture Notes in Computer Science, pages 110-125. Springer Berlin / Heidelberg.

[Boyle and Greenberg, 2005] Boyle, M. and Greenberg, S. (2005). The language of privacy: Learning from video media space analysis and design. A CM Trans. Comput.-Hum. Interact., 12(2):328-370.

[Boyle et al, 2008] Boyle, M., Neustaedter, C, and Greenberg, S. (2008). Privacy factors in video-based media spaces. In Harrision, S., editor, n Media Space: 20+ Years of Mediated Life, pages 99-124. Springer.

[Brands and Paquin, 2010] Brands, S. and Paquin, C. (2010). U-prove cryptographic specification vl.0. Technical report, Microsoft Corporation.

[Camenisch and Lysyanskaya, 2001] Camenisch, J. and Lysyanskaya, A. (2001). 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, EUROCRYPT '01, pages 93-118, London, UK. Springer-Verlag.

[Chaum, 1985] Chaum, D. (1985). Security without identification: transaction systems to make big brother obsolete. Commun. ACM, 28(10):1030-1044.

[Chaum, 1981] Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. Commun. ACM, 24(2):84-90.

[Damgard, 1990] Damgard, I. B. (1990). Payment systems and credential mechanisms with provable security against abuse by individuals. In Proceedings on Advances in cryptology, CRYPTO '88, pages 328-335, New York, NY, USA. Springer-Verlag New York, Inc.

[Danezis et al., 2003] Danezis, G., Dingledine, R., and Mathewson, N. (2003). Mixmin-ion: design of a type iii anonymous remailer protocol. In Security and Privacy, 2003. Proceedings. 2003 Symposium on, pages 2-15.

[Dingledine et al, 2004] Dingledine, R., Mathewson, N., and Syverson, P. (2004). Tor: the second-generation onion router. In Proceedings of the 13th conference on USENIX Security Symposium - Volume 13, SSYM'04, pages 21-21, Berkeley, CA, USA. USENIX Association.

[Pfitzmann, 1990] Pfitzmann, A. (1990). Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz (Services Integrating Communication Networks with Participant-verifiable Privacy). IFB 234, Springer-Verlag, Heidelberg.

[Fischer et al., 2012] Fischer, L., Heupel, M., Bourimi, M., Kesdogan, D., Gimenez, R. (2012). Enhancing Privacy in Collaborative Scenarios Utilising a Flexible Proxy Layer. Proceeding of the International Confernce on Future Generation Communication, London, UK.

[Fischer and Eckert, 2008] Fischer, L., Eckert, C. (2008). 50_6 Ways to Track Your Lover. Proceedings of the WiVeC Symposium.

[Fischer-Huebner, 2001] Fischer-Huebner, S. (2001). 4- Privacy-Enhancing Technologies, Lecture Notes in Computer Science. Springer.

[Fraunhofer Institut fur Sichere Informationstechnologie, 2008] Fraunhofer Institut fur Sichere Informationstechnologie (2008). Privatspharenschutz in soziale-netzwerke- plattformen. Fraunhofer SIT, Darmstadt.

[Gindin, 2009] Gindin, S. (2009). Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears. Nw J Tech & Intell Prop.

[Gross et al., 2003] Gross, T., Wirsam, W., and Graether, W. (2003). Awarenessmaps: visualizing awareness in shared workspaces. In CHI 'OS: CHI 'OS extended abstracts on Human factors in computing systems, pages 784-785, New York, NY, USA. ACM Press.

[Gutwin, 1997] Gutwin, C. (1997). Workspace Awareness in Real-Time Distributed Groupware. PhD thesis, The University of Calgary.

[Haake et al., 2004a] Haake, J., Schummer, T., Haake, A., Bourimi, M., and Landgraf, B. (2004a). Supporting flexible collaborative distance learning in the cure platform. In System Sciences, 200Jh Proceedings of the 37th Annual Hawaii International Conference on, page 10 pp.

[Haake et al., 2004b] Haake, J. M., Haake, A., Schummer, T., Bourimi, M., and Landgraf, B. (2004b). End-user controlled group formation and access rights management in a shared

workspace system. In CSCW '04'. Proceedings of the 2004 ACM conference on Computer supported cooperative work, pages 554-563, Chicago, Illinois, USA. ACM Press.

[Hildebrandt, 2008] Hildebrandt, M. (2008). Profiling and the rule of law. Identity in the Information Society, 1:55-70. 10.1007/sl2394-008-0003-l.

[Karatas et al., 2013] Karatas, F., Bourimi, M., Barth, T., Kesdogan, D., Gimenez, R., Schwittek, W., and Planaguma, M. (2012). Considering Interdependent Protection Goals in Domain-Specific Contexts: The di.me Case Study. Proceedings of the 10th IEEE International Conference on Pervasive Computing and Communications.

[Karatas et. al., 2013] Fatih Karatas, Marcel Heupel, Mohamed Bourimi, Dogan Kesdogan, Sophie Wrobel (2013). Communication anonymity with balancing end-users' and business' needs in decentralized social networking. Proceeding of the 10th International Conference on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA.

[Kellermann, 2008] Kellermann, B. (2008). Collaborative elearning with blues'n prime application prototype v3.

[Lambropoulos et al., 2012] Lambropoulos, N., Faulkner, X. & Culwin, F. (2012). Supporting Social Awareness in Collaborative E-learning. The British Journal of Educational Technologies (BJET), Volume 43, Issue 2, pages 295–306, March 2012.

[Labitzke et al., 2011] Labitzke, S., Taranu, I., Hartenstein, H. (2011). What your friends tell others about you: Low cost linkability of social network profiles. In: Proceedings of the 5th International ACM Workshop on Social Network Mining and Analysis, SNAKDD 2011. ACM.

[Liesebach et al., 2011] Liesebach, K., Franz, E., Stange, A.-K., Juschka, A., Borcea-Pfitzmann, K., Bottcher, A., and Wahrig, H. (2011). Collaborative E-Learning. In Camenisch, J., Leenes, R., and Sommer, D., editors, Digital Privacy, volume 6545 of Lecture Notes in Computer Science, pages 657-677. Springer Berlin / Heidelberg. 10.1007/978-3-642-19050-6_24.

[Narayanan and Shmatikov, 2009] Narayanan, A. and Shmatikov, V. (2009). De-anonymizing social networks.

[Needham, 2010] Needham, R. (2010). Security Engineering: A Guide to Building Dependable Distributed Systems. Second Edition. Chapter 9: Multilateral Security, Wiley.

[Palen and Dourish, 2003] Palen, L. and Dourish, P. (2003). Unpacking "privacy" for a networked world. In CHI 'OS: Proceedings of the SIGCHI conference on Human factors in computing systems, pages 129-136, New York, NY, USA. ACM Press.

[Pötzsch et al., 2011] Pötzsch, S. Borcea-Pfitzmann, K., Hansen, M., Liesebach, K., Pfitzmann, A., and Steinbrecher, S. (2011). Requirements for Identity Management from the Perspective of Multilateral Interactions. In: Digital Privacy: PRIME - Privacy and Identity Management for Europe, volume 6545 of Lecture Notes in Computer Science, pages 597–614. Springer.

[Rannenberg, 1994] Rannenberg, K. (1994). Recent Development in Information Technology Security Evaluation The Need for Evaluation Criteria for multilateral Security. In: Security and Control of Information Technology in Society Proceedings of the IFIP TC9/WG 9.6 Working Conference, pp. 113-128, published by North-Holland, Amsterdam.

[Rannenberg, 2001] Rannenberg, K. (2001). Multilateral security a concept and examples for balanced security. In: NSPW '00 - Proceedings of the 2000 workshop on New security paradigms.

[Sailer, 1998] Sailer, R. (1998). An Evolutionary Approach to Multilaterally Secure Services in ISDN / IN. Proceedings of the Seventh International Conference on Computer Communications and Networks, Lafayette (Louisiana), pp. 276-283.

[Schwarte et. al., 2013] Schwarte, P., Bourimi, M., Heupel, M., Kesdogan, D., Gimenez, R., Wrobel, S., Thiel, S. (2013). Communication anonymity with balancing end-users' and business' needs in decentralized social networking. Proceeding of the 10th International Conference on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA.

[Sweeney, 2002] Sweeney, L. (2002). Achieving k-anonymity privacy protection using generalization and suppression. Int. J. Uncertain. Fuzziness Knowl.-Based Syst., 10(5):571-588.

[Tang et. al., 1994] Tang, J. C, Isaacs, E. A., and Rua, M. (1994). Supporting distributed groups with a montage of lightweight interactions. In CSCW '94: Proceedings of the 1994 ACM conference on Computer supported cooperative work, pages 23-34, NY, USA. ACM.

[The National Campaign, 2008] The National Campaign (2008). Sex and tech-results from a survey of teens and young adults.

[Westfeld, 1999] Westfeld, A. (1999). Steganography and Multilateral Security. In Multilateral Security in Communications Vol. 3: Technology, Infrastructure, Economy. Addison-Wesley-Longman, Munich.

[Wolf et. al., 2000] Wolf, G., Pfitzmann, A. (2000). Properties of protection goals and their integration into a user interface. Computer Networks, Volume 32, Issue 6, Pages 685-700.

[Woolf, 2007] Woolf, B. P. (2007). Building Intelligent Interactive Tutors: Student-centered strategies for revolutionizing e-learning. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

[Wrobel et al., 2013] Sophie Wrobel, Mohamed Bourimi, Marcel Heupel, Fabian Herrmann, Massimo Valla (2013). Towards a minimal framework considering privacy and data protection goals for social networking platform providers The Power of Information Conference '13 Extended Abstracts, Brussels (2013).