Enhancing Usability of Privacy-Respecting Authentication and Authorization in Mobile Social Settings by Using Idemix (in the context of the EU FP7 di.me Project)

Mohamed Bourimi, Marcel Heupel, Dogan Kesdogan and Thomas Fielenbach

Information Systems Institute (Fachbereich 5 - Wirtschaftsinformatik)
IT Security Management Group
57076 Siegen, Germany
{bourimi,heupel,kesdogan,fielenbach}@fb5.uni-siegen.de

Abstract. Authentication and authorization are an essential part of any system allowing for information sharing and social interaction. Especially in such social settings where mobile devices with restricted capabilities and new possibilities (e.g. screen size, ease of localization) are used, there is an increasing need for providing privacy-respecting integrity and access permission mechanisms by considering trade-offs related to usability aspects. In this paper we show how the usability of authentication and authorization related interaction can be enhanced in mobile social settings. This is carried out in our case by using proof-based anonymous credential systems such as Idemix. The requirements analysis is based on various case studies in building collaborative systems and oriented to the needs of the upcoming EU FP7 funded project di.me. We also present the prototypic implementation and future work directions.

Identity management; idemix; authentication and authorization; security vs. usability; social interaction

1 Introduction

Due to the rapid evolution of computing systems and sinking costs of connecting them to the Internet, mobile devices are increasingly being used in different sectors of our leisure and professional life. Recently, Ericsson estimated mobile subscriptions have hit 5 billion and the Wi-Fi Alliance and Wakefield Research estimate that only in this year 216 million devices will be sold from which 82 million provide Wi-Fi functionality [1]. Thereby, these devices offer new possibilities of situated interaction and are therefore often also used in social settings. Such mobility (mostly with continuous connectivity) brings new challenges for security and privacy in ubiquitous and pervasive computing. However, preserving the users' security and privacy in social settings is the most often-cited point of critique of mobile and ubiquitous computing [2]. Even though anonymization

and data minimization mechanisms (i.e., removing sensitive data like names or addresses from social network accounts etc.) are provided, the users can be re-identified across distinct high popular social networks like Facebook, Flickr, MySpace or Twitter with an error rate of just 12% such as recently shown in [3]. Linkability and the building of user profiles based on social interaction traces might be the starting point for potential man-in-the-middle attacks.

With respect to the different capabilities and restrictions of modern mobile devices (e.g. smart-phones and tablet PCs), addressing security and usability aspects becomes crucial. Experts from various research communities believe that there are inherent trade-offs between security and usability to be considered [4][5][6]. Indeed, a good example for trade-offs between security (privacy) and usability or maybe good design is Apple's iPhone. Even tough it was less secure than RIM's BlackBerry or devices using Microsoft's Windows Mobile [7] in older releases, customers were still switching to it and Yahoo announced to focus in its mobile program on the support of iPhone and abandoned its BlackBerry smartphone application [8].

In this paper we focus on the usability of authentication and authorization related interaction and show how both can be enhanced in mobile social settings. We use thereby a cutting-edge proof-based anonymous credential system called Idemix. Latter was developed at IBM Research Zurich and meets our needs and requirements identified in the EU FP7 funded project di.me[1]. Since di.me is targeting the involvement from 500 up to 10000 users, possible authentication and authorization interaction design becomes crucial and affects therefore the usability of the developed applications. Our prototypic implementation on different Android smart-phones and tablets showed the feasibility of our approach.

We first present related work in Section 2, then we address our problem and requirements analysis based on case studies and current projects in Section 3. In section 4 we present our approach as well as implementation details, before we finish with our conclusion and an outlook about ongoing and future works in Section 5.

2 Related Work

Social interaction is mostly supported by different categories of collaborative systems and social software. Such systems have to fulfill multi-user requirements and are consequently characterized by complex scenarios supporting those requirements in the respective domain.

Often, this complexity is reflected in the user interface (UI) which becomes crucial for mobile applications deployed on mobile devices with limitations in the screen space [5][6]. According to Shneiderman et al., *"an extrapolation of current trends leads to the suggestion that most computer-based tasks will become collaborative because just as most work environments have social aspects"* [5]. Thus, software systems and applications supporting social interaction are considered as

[1] This work has been funded by the EC(FP7/2007-2013) under grant agreement no 257787.

socio-technical systems in the Computer-Supported Cooperative/Collaborative Work (CSCW) as well as Human-Computer Interaction (HCI) research fields [9][5]. Mostly, end-users have to balance functionality and their security/privacy preferences by using several mechanisms built into the system. Authentication and authorization are the main mechanisms such system has to achieve, ideally without affecting the usability of the application. Usability related issues are also discussed in-depth by security and usability researchers in [4] and [10] from both; theoretical and practical perspectives. Researchers from all cited research fields generally agree on that security and privacy issues arise due to the way systems are designed, implemented, and deployed [4][6][5]. Trade-offs between security and other (non-)functional requirements are well-described in tremendous lot of classical literature in the corresponding research communities. Nevertheless, the current state of the art leaves room for considerable improvement how such systems can support an usable and secure user experience as we show in the following.

Common practices for authentication are knowledge based authentication mechanisms (by using a shared secret, e.g. password) or biometric approaches where unique characteristics of the human body are used to prove a persons' identity. The widely used password authentication is in general a good approach under the prerequisite that a secure password is used. In general passwords are notoriously weak, mostly because of limitations of human information-processing and/or limited capabilities of the respective mobile device. Even though some organizations are enforcing different practices (e.g. changing passwords periodically), applying good practices known from the desktop world remain crucial on a mobile keyboard and makes the most paranoid security professional rethink their password strategy [10]. A contribution from the usability field to enhance authentication is e.g. the usage of graphical password facilities. An example is the usage of pass-faces for graphical authentication in Android smart-phones to unlock the main screen. However also those approaches have been proven to be not secure enough e.g. due to the smudge traces that can emerge on the screen surface. A recent publication showed that is really easy to guess the right pattern and break such authentication system [11]. Biometrics also allows for enhancing authentication but are still *"classified as unreliable because human beings are, by their very nature, variable"*[4][12]. In addition, they are still not popular and relatively unused today like smart cards and (multifunction) USB tokens. This is especially true for mobile devices such as smart-phones and tablets.

Related to authorization, most systems need the interaction of the end-users at least in form of confirmations. The challenges increase if (lay) users are asked to set access rights for others, delegate rights, or manage their own security and privacy preferences. In the context of this work, the EU Project PICOS (Privacy and Identity Management for Community Services) [13] represents a good and current example. The *"2010 First Community Prototype Lab and Field Test Report D7.2a"* [14] cites that users had problems to use the PICOS privacy manager on mobile devices (Nokia MusicExpress 5800). Notifications and (automatic) advisory might lead to actions which the user finds intrusive or annoying

in some cases (such as in the well-known case of Windows pop-ups or MSWord's paper-clip). Especially in collaborative applications as socio-technical systems, this will affect the psychological acceptance of the application which leads to not using security and privacy mechanisms. This mostly results in expensive change requirements affecting the technical realization of mobile applications [4][15]. Indeed, people involvement varies and the usage can range from occasional to frequent according to a given setting and circumstances. The same socio-technical system can lead to different evaluation results in different social environments [9].

For both; authentication and authorization, cryptography is an established used mechanism for increasing confidentiality and integrity of exchanged data. However, a total security or privacy provision is an illusion [2] because current approaches are not able to avoid at least threats and attacks e.g. emerging from loosing devices or based on physical access to them [10]. Approaches mostly only focus on hindering such attacks or making them difficult. Security and usability research for developing usable (psychologically acceptable) security mechanisms is a young research field which depends on the context in which those mechanisms have to be used [4]. Because of this and many facts cited above, we argue that security and privacy design by considering usability is specific to the project context and we thus analyze authentication and authorization requirements in this paper based on concrete di.me requirements by considering lessons learned from previous projects and good practices cited in standard literature.

3 Requirement Analysis

3.1 Requirements based on previous experiences with collaborative platforms

In this sub-section, we introduce the CURE (Collaborative Universal Remote Education) platform as a basis for a part of our requirements analysis on dealing with authentication and authorization in social (collaborative) settings. CURE supports self-organized learning and a wide range of learning scenarios (i.e. collaborative exercises, tutor-guided groups with collaborative exercises, virtual seminars, virtual labs, collaborative exam preparation) at the German Distance Learning University [16]. CURE is used now in different fields and hence covering CSCW, and not only CSCL, scenarios. Since fall 2004, CURE is an integral part of the virtual learning space of the FernUniversät in Hagen, is available under an open source license, and has currently more than 2500 registered users. During this long time period the CURE designers received valuable user feedback also concerning privacy, awareness, and usability concerns and shared these with us.

Choosing the CURE platform is due to different reasons meeting our argumentation in this paper: (1) CURE can be seen as a representative general-purpose collaborative system and its conceptual design is common to a wide range of existing collaboration platforms and systems (provides Wiki, forums, uploads, mail and chat etc.), and (2) the improvement needs in CURE we were

informed about from our partners over many years of usage have a valid character for many systems supporting social interaction. CURE uses a room metaphor to model shared workspaces for groups. A virtual key metaphor is used to determine access rights and possible interactions in rooms. Users who have keys to a given room can form groups in that room in order to cooperate and work with each other. The structuring of collaborative environments is carried out by connecting individual rooms. The virtual keys of a user determine their possible interactions in a given room. Users with sufficient rights, such as for creating adjacent rooms or passing on virtual keys, can adapt the collaborative environment according to their needs. So, end-users are able to manage and control access rights to their rooms, and can flexibly organize their work themselves. Dynamic groups can be formed without privileged users. End-users (instructors, tutors, students etc.) are able to form groups (1) by key assignment, (2) by invitation, (3) with free enrollment, and (4) enrollment confirmed by the members of the respective groups [17].

Some of the detected privacy issues were solved in the work described in [18] (related to real-identity issues in CURE). In the context of this paper, however, some of the open issues are still existing and are closely related with authentication and authorization. For instance, even though a workflow for easing key creation and configuration (i.e. time validity) as well as key assignment is provided; there are still a lot of possible enhancements from which we enumerate a few in the following:

1. E-learing platforms (e.g. CURE, BSCW or Moodle etc.) mostly represent a real-identity collaboration system and users have to use their real names (instructors) or their university pseudonyms (based on students Ids) in order to access the materials.
2. Creation, configuration, and assignment of access rights remains difficult for lay users even though online help and documentation is available. If a user asks other users for rights in their rooms (confirmed enrollment), the latter has to check asked rights and agree. Experiences show that this task generates many situations that affect security, privacy, and trust in such environments. For example, (1) requests are hasty agreed without checking their rights, (2) agreed by reducing their rights (by disappointing the requesting user), or (3) delayed in order to check them properly (by blocking the cooperation). People are task-oriented and might be disturbed with such requests also in the case of group building by invitation or key assignment[4].

3.2 Requirements based on di.me scenarios

di.me aims at providing a user-ware tool integrating all personal data in a personal sphere by a single, user-controlled point of access. This tool will run on the user's (mobile) devices, and rely on scaleable peer-to-peer (P2P) communication in order to avoid external storage of personal data as far as possible and to enhance data portability. External services (e.g. web-communities, enterprise systems) will be integrated via gateways. Communication to individuals and services will make use of digital faces (representing partial identities), i.e. user data

selected for a particular purpose and context. A work package related to our work has to provide an open trust, privacy, and security infrastructure which enables the end-users to securely use their personal data. For this, di.me targets to leverage and elaborate concepts such as digital faces as well as anonymity at the application level (anonymous user-controlled identity management; IdM) and supporting secure mechanisms at the network level, too (e.g. by supporting TOR anonymity).

In summary, the first analysis of selected di.me scenarios identified the need for usability enhancements which are very similar to identified needs for CURE in the previous sub-section related to authentication and authorization. In our case, Idemix represents the best possibility to fulfill di.me's requirements without additional development costs. Idemix is licensed for non commercial usage in EU projects since it was and is still being developed and used in projects funded by the EU (Prime and PrimeLife). Such proceeding of using results from previous EU funded projects is also strategically preferred by the EU. However, Idemix represents a cutting-edge framework in comparison to other solutions like U-Prove [19].

First usage of Idemix on mobile smartphones showed the need for performance enhancements. The evaluation results showed that requests could reach 20 seconds according to the proofs complexity in combination with enabling TOR-Anonymity [20]. This could negatively affect the intended user trials since di.me targets the involvement of a very large testers community (from 500 up to 10000 as mentioned before). Since performance is seen as a quality of service requirement from the usability perspective and an availability requirement from the security point of view[2], we performed a deep performance evaluation of Idemix usage in those scenarios. For accuracy, "Developing a prototype reference implementation of an IdM system for mobile end-user devices is one of the high-level requirements of di.me" which implicates the following concrete requirements:

1. the IdM to be developed or integrated by using Idemix has to be deployable on mobile platforms without affecting usability acceptance for instance in terms of interaction design or performance (response times) by enhancing selected authentication and authorization if possible in order to not delay or block social interaction **(R1)**,
2. and thereby with considering the end-users' security and privacy needs e.g. for anonymity, un-linkability and so on **(R2)**.
3. Because di.me wants to leverage P2P possibilities, a realistic mobile collaborative scenario implementation has to be provided and evaluated on the target mobile platform for R1 and R2 **(R3)**.

[2] The reader may remember the security triangle: confidentiality, integrity, and availability.

4 Our Approach

To fulfill the requirements R1-R3 we identified in Section 3, we analyzed selected di.me scenarios and use cases with respect to security, privacy, and trust. In the following, we first provide background information to Idemix, then we show how Idemix can be used for fulfilling R1-R3 in di.me scenarios, and we finally describe our implementation.

4.1 Idemix background information

Idemix is an anonymous credential system, developed by the research group led by Jan Camenisch at IBM Research Zurich [21]. It enables to perform anonymous authentication between users and/or service providers and as well supports accountability of transactions [22]. An Idemix credential is obtained from an issuing authority, attesting to the users attributes such as birth date or access rights and allows for various protocols and mechanisms cited in standard literature (i.e. property proofs, usage limitation, revocation of credentials, revocation of anonymity, verifiable encryption). The main protocols performed, are the credential issuance and the show proof protocol which are using the Camenisch-Lysyanskaya signature scheme [23],[24]. With Idemix, one could prove to Amazon being over 18 when buying games having such restriction without disclosing the accurate birthday (only in theory, because Amazon does not yet support idemix). Furthermore, one can pay and receive the respective game and only the delivery service (e.g. DHL or UPS) will be able to see his/her address etc. The following Figure 1 illustrates the Idemix collaboration in a CURE-based scenario. Alice and Bob are each interactively creating a credential with the certificate authority (CA). The issuing CA signs this credential with its private key, so it can easily be verified using the issuerâs public key. It also contains a pseudonym, that was generated from the users master key, to bind the users identity to the credential [25]. As shown in Figure 1, Alice and Bob are communicating with each other directly, over the XMPP server (eJabberd), or they can collaborate with other users using a common server (here CURE). In both cases, the communication is performed completely anonymously. They are also completely free to decide if they only want to use one of both mechanisms. To authenticate and authorize them for certain actions, users can create customized, context dependent âproofsâ (which are verifiable statements about attributes) with their credentials. In contrast to privacy enhancing technologies sending pseudonym certificates to a given verifier, the credential itself is never revealed. This makes profile building based on attribute inferring tedious. The computed proof (such as "I am older than 18" or "working in the automotive industry") has the characteristic to be zero-knowledge, and thereby allows un-linkable, selective disclosure of such attested credential attributes while not revealing others (realizing so different di.me's digital faces). In our context, users can use such a proof to authenticate themselves to each other or to gain authorized access to the CURE server.

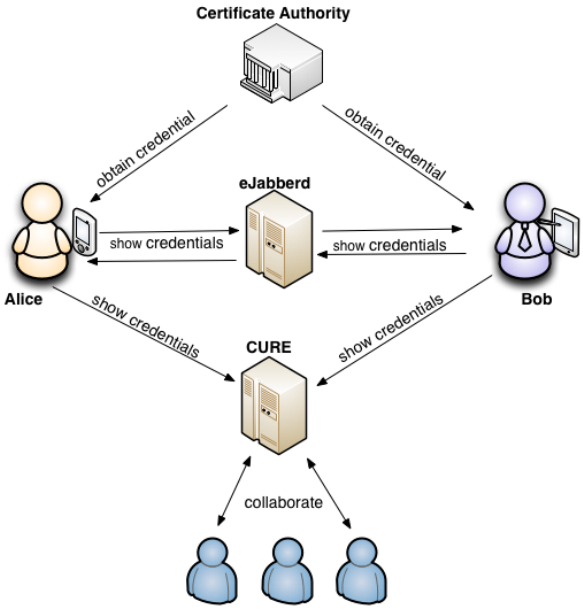

Fig. 1. Idemix CURE-based collaboration scenario

4.2 Our approach and its usage for implementation the di.me Conference Scenario

From the previous explanations, Idemix represents a perfect starting point for automating privacy-enhancing authentication and authorization in the background meeting so R1 and R2. By allowing for background authentication and authorization, a good performance could be reached since designing interaction not expecting user intervention becomes possible. Indeed, the CA could provide needed acknowledgements for access permission enforcement without waiting on user interaction in the UI. However, this needs a pre-defined set of attributes which are allowed to be included into automatic generated proofs. For this we provide a separate UI allowing for combining attributes and bundling them to a single proof, that have to be shown in order to obtain a permission. For meeting R3, we implemented the so-called *Conference Scenario* in which the attendees have the option to publish some selected personal contact information on a conference shared space (CURE website in our prototypic implementation). The other attendees can browse the information and could e.g send contact requests (i.e. requesting further materials such as slides or further contact data). When publishing such information, it is possible to conceal some information and make them only available for people in possession of a particular attribute (e.g. the email address is only visible to people working in the automotive industry). The access to the materials is automatically performed in the background without explicit users intervention in UIs because Idemix allows for this. Since all atten-

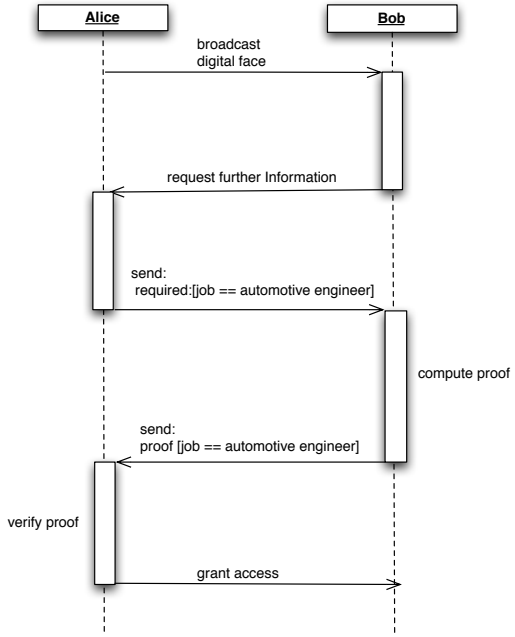

Fig. 2. Sequence diagram of the broadcasting process

dees receive a special credential proving they are registered participants of the conference, authentication is also carried out in the same way, namely, transparently in the background without any end-user intervention. Besides the public section of the website, where everybody can publish contact information, there are several virtual conference rooms and discussion forums. Attendees can e.g. create their own private chat rooms. If another attendee likes to join this chat room, he/she has to prove that e.g. his job is "automotive engineer". Since EU mobile network providers do not allow clients to use different dynamic IPs such as in Australia, becoming a P2P server and client at the same time has to be modeled otherwise in our case. For simulating P2P social settings we used an eJabberd XMPP Server [26]. It was set up in our lab tests in an ad-hoc manner (by directly setting its WiFi IP via an UI provided at the level of the mobile client application). A global conference room was used to broadcast general information to the conference and all clients were signed-in through the duration of the conference. Separate conference rooms for each session, track or interest group can also be set up in ad-hoc manner by the end-users. Since all clients connected to a conference room (global or concern-related) receive the XMPP messages going to this room, end-users are able to react on information they are interested in (represented in a messages ListView in the client UI such as "Further contact data available for engineers"). If an interested attender clicks on a given message, a request is sent to the broadcaster. Thereby Idemix is act-

ing in the background for authentication as well as for authorization. Figure 2 shows such interaction in form of a sequence diagram for a potential interaction between Bob and Alice. As depicted in the sequence diagram the following steps are carried out:

Broadcasting personal information To publish personal information all clients are joining a hidden conference room (group chat). In this channel users can broadcast messages, and as well browse the messages of the other users. The client application parses and formats the messages in the group chat in order to make it more comfortable for the user to browse them on the mobile device.

Automated proofs If the client tries to access a document that is restricted to users with a certain attribute, a challenge is send to the client, asking it to proof a certain value of an attribute (e.g. attribute JOB == "engineer"). If the necessary credential exists, the client now automatically creates a fitting proof statement and sends it to the requester. The latter now verifies that proof and grants access.

4.3 Implementing details

To verify the feasibility of our approach for our scenario we implemented an Android-based prototype as well as a server-side supporting CURE or eJabberd servers. The client mobile application is able to perform the two main protocols of Idemix ("Get Credential" and "Show Proof") either via XMPP or via XML-RPC requests. This section should give a short overview about the implementation details of our concrete requirements.

Client/server architecture In our approach we are using two different servers; the credential issuance server, where users obtain their conference credential as well as a collaboration server. The Certificate Authority (CA) is written in Java and implementing an XML-RPC servlet, so we can send XML-RPC requests to perform the credential issuance protocol. The server supports full Idemix capabilities, so it is also possible to show proofs to the server. This can be used, for example if an additional authentication is needed in order so sign a new credential. The collaboration can be in our case a CURE server or any eJabberd server which can be accessed via WiFi. It also allows us to easily fulfill requirements (we are not focusing on in this paper) like group awareness and real time communication. As mentioned before, users can create their own chat rooms and can define certain restrictions other users have to fulfill in order to join. At the moment there is just password protection, but in order to obtain the password, users can send an Idemix proof to the owner.

Client-to-client communication In order to be able to show proofs to other users, the clients are connected to an XMPP server. Therefore we implement a

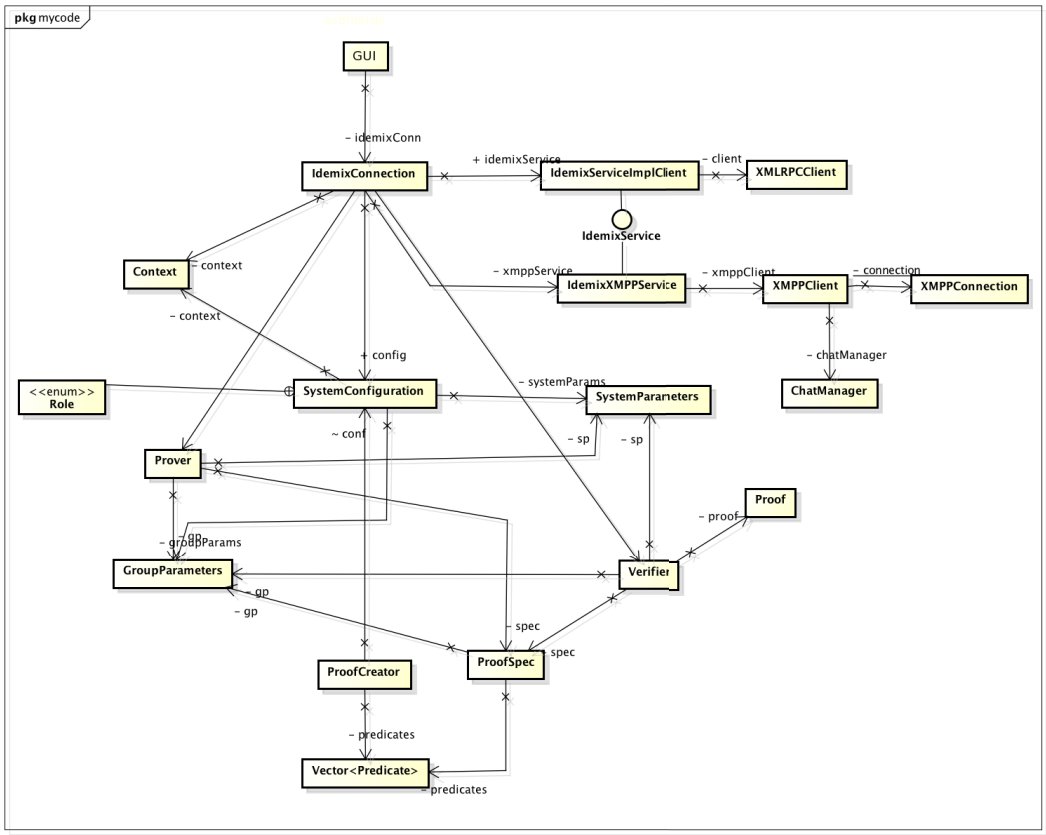

Fig. 3. Client class diagram of the Android-based prototype

custom XMPP extension, allowing us to send customized ,"Idemix messages" (as we described above for "Further data is available" or similar messages) to be able to perform the Idemix protocols. In our current prototype the XMPP server is installed on a secure machine, maintained by the conference organizer. Additionally the transmitted traffic is TLS encrypted to ensure confidentiality of communications. The client class diagram allowing for XMPP and also XML-RPC functionality is shown in Figure 3.

5 Conclusion and Future Work

In this paper, we showed how authentication and authorization can be enhanced by using the Idemix system. Since Idemix is a proof-based identity mixer, it allows for automating some scenarios by providing un-linkable anonymity. The feasibility of our approach was demonstrated by implementing the di.me Conference Scenario which enables participants to transparently exchange data in

the background without the need for explicit interaction (e.g. in UIs). This is possible since Idemix assesses that the attendees fulfill some attributes in the background (i.e. required affiliation) and provide access without disturbing the information provider. The same is carried out for transparent authentication in the background. Furthermore, our Android-based client implementation leverages P2P capabilities to enhance the security and privacy explicitly required in various di.me scenarios. With this, our approach presents a new solution which is to our best knowledge not addressed in related work. Future directions intend enhancing the P2P capabilities by integrating the P2P server on the same client. So, there will be no need for providing ad-hoc trustable P2P servers in order to support our scenarios such as described in the Conference Scenario. Wi-Fi Direct in combination with server-less XMPP (see also [27]) might help to perform flexible, secure near range exchange of data. Other efforts are also followed by our usability experts to provide a usable interface for defining attribute-based proofs (for lay users without Idemix background, too). However, Idemix does not allow for building contradictory attribute combinations, so that testers were able in our lab tests to create proofs without big cognitive load.

Acknowledgment

The authors would like to thank Jan Camenisch and his group in IBM Zurich as well as Ibrahim Armac from the department of computer science, RWTH Aachen University for answering our questions and supporting us by porting the Java-based Idemix reference implementation to Android. Thanks are also due to our partners from the FernUniversitaet in Hagen for sharing their experiences and helping us for adapting the open source CURE code for our validation purposes.

References

1. Wi-Fi Alliance, "Wi-Fi Direct." [Online]. Available: http://www.wi-fi.org/Wi-Fi_Direct.php
2. J. I. Hong and J. A. Landay, "An architecture for privacy-sensitive ubiquitous computing," in *MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*. New York, NY, USA: ACM, 2004, pp. 177–189.
3. A. Narayanan and V. Shmatikov, "De-anonymizing social networks," 2009.
4. L. Cranor and S. Garfinkel, *Security and Usability*. O'Reilly Media, Inc., 2005.
5. B. Shneiderman, C. Plaisant, M. Cohen, and S. Jacobs, *Designing the User Interface: Strategies for Effective Human-Computer Interaction*, 5th ed. Shneiderman, March 2009.
6. M. Boyle, C. Neustaedter, and S. Greenberg, "Privacy factors in video-based media spaces," in *n Media Space: 20+ Years of Mediated Life*, S. Harrision, Ed. Springer, 2008, pp. 99–124.
7. eWeek.com, "Research in motion tops security assessment," http://www.eweek.com/c/a/Mobile-and-Wireless/Research-In-Motion-Tops-Security-Assessment-783185/, May 27 2009.

8. TechCrunch, "Yahoo mobile abandons its smartphone app to focus on the iphone," http://www.techcrunch.com/2009/05/18/yahoo-mobile-abandons-its-blackberry-app-to-focus-on-the-iphone/, May 18 2009.
9. T. Gross and M. Koch, *Computer-Supported Cooperative Work (CSCW)*. Oldenburg, 2007.
10. H. Dwivedi, C. Clark, and D. Thiel, *Mobile Application Security*. The McGraw-Hill Companies, 2010.
11. A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," 2010.
12. K. Kryszczuk and A. Drygajlo, "Credence estimation and error prediction in biometric identity verification," *Signal Process.*, vol. 88, no. 4, pp. 916–925, 2008.
13. PICOS EU Project Homepage, "Privacy and identity management for community services," http://www.picos-project.eu, 2010.
14. PICOS TEAM, "PICOS Public Deliverables Site," http://picos-project.eu/Public-Deliverables.29.0.html, January 2010.
15. V. Lee, H. Schneider, and R. Schell, *Mobile Applications: Architecture, Design, and Development*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2007.
16. J. M. Haake, T. Schümmer, A. Haake, M. Bourimi, and B. Landgraf, "Supporting flexible collaborative distance learning in the cure platform," in *Proceedings of the Hawaii International Conference On System Sciences (HICSS-37)*. IEEE Press, January 5-8 2004.
17. J. M. Haake, A. Haake, T. Schümmer, M. Bourimi, and B. Landgraf, "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*. Chicago, Illinois, USA: ACM Press, November 6-10 2004, pp. 554–563.
18. M. Bourimi, F. Kühnel, J. M. Haake, D. el Diehn I. Abou-Tair, and D. Kesdogan, "Tailoring collaboration according privacy needs in real-identity collaborative systems," pp. 110–125, 2009.
19. S. Brands and C. Paquin, "U-prove cryptographic specification v1.0," Microsoft Corporation, Tech. Rep., March 2010.
20. M. Heupel, "Porting and evaluating the performance of idemix and tor anonymity on modern smartphones," Master's thesis, University of Siegen, Dec. 2010. [Online]. Available: http://www.uni-siegen.de/fb5/itsec/publikationen/da-heupel.pdf
21. "IBM Research Zurich, Identity Governance." [Online]. Available: http://www.zurich.ibm.com/security/idemix
22. J. Camenisch and E. Van Herreweghen, "Design and implementation of the idemix anonymous credential system," in *CCS '02: Proceedings of the 9th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2002, pp. 21–30.
23. J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation," pp. 93–118, 2001.
24. ——, "A signature scheme with efficient protocols," pp. 268–289, 2003.
25. IBM Research Report, "Specification of the identity mixer cryptographic library," IBM Research, Zurich, Switzerland, Tech. Rep., April 2010.
26. EJabberd, "eJabberd, the Erlang Jabber/XMPP daemon," http://www.ejabberd.im/, January 2010.
27. "Xep-0174: Serverless messaging," http://xmpp.org/extensions/xep-0174.html, November 2010.