Enhancing Multilateral Security in and by Reputation Systems

Sandra Steinbrecher

Technische Universität Dresden, Fakultät Informatik, D-01062 Dresden, Germany,
steinbrecher@acm.org

Abstract. With the increasing possibilities for interaction between Internet users exceeding pure communication, in multilateral security the research question arises to rethink and extend classical security requirements. Reputation systems are a possible solution to assist new security requirements. But naturally also reputation systems have to be designed in a multilateral secure way. In this paper we discuss both multilateral security by and in reputation systems. An overview on the possibilities how such systems could be realised is given.

1 Introduction

The Internet offers its users numerous possibilities to interact with each other. Interactions cover various fields of interest for many people, e.g. trades via marketplaces like eBay[1] or online games like Second Life[2].

For interactions security requirements and trust issues are important. An interaction partner first wants to know what to expect from others and then wants to trust in the fulfilment of his expectations. Usually only users who fulfil these expectations are seen as trustworthy in the future. Social scientists and theoretical economists model the problem whether two interaction partners should place trust in each other as a so-called trust game [4, 9].

On the Internet users often only interact once with each other. To help new interaction partners to estimate the others' behaviour reputation systems have been designed and established to collect the experiences former interaction partners made [20]. A very-popular example of a reputation system is implemented by eBay. As marketplace eBay offers its members the possibility to sell and buy arbitrary objects. The exchange of object and money usually is done by bank transfer and conventional mail. Many of these exchanges are successful, but unfortunately some are not. For this reason a reputation system collects the experiences sellers and buyers make. After every exchange they may give comments or/and marks to each other that are added to the members' public reputations (usually together with the annotator and the exchange considered as context information).

Currently the vision arises to establish stand-alone reputation systems that collect information from various interactions and in various contexts and also

[1] http://www.ebay.com/ (last visited Jan. 09)
[2] http://www.secondlife.com/ (last visited Jan. 09)

to make reputation information in different systems interoperable [13]. For the latter there is already an OASIS group[3] established.

For the collection of large reputation profiles for Internet users privacy becomes an important issue. Reputation systems often collect information about who interacted with whom in which context. Such information should be protected by means of technical data protection to ensure users' right of informational self-determination [16].

Privacy-enhancing user-controlled identity management [8, 7] like PRIME[4] assists users platform-independent in controlling their personal data in various applications and selecting pseudonyms appropriately depending on their wish for pseudonymity and unlinkability of actions.

Reputation needs not be linked to real name but can be assigned to a pseudonym as well. But the interoperability of a reputation system with a user-controlled privacy-enhancing identity management needs a privacy-respecting design of reputation systems while keeping the level of trust provided by the use of reputations.

In section 2 we give an overview of the security requirements a reputation system should resp. can help to fulfil for interactions. Based on this analysis in section 3 we explain how reputation systems can be realised in a multilateral secure way themselves. Especially we give a categorisation of building blocks able to fulfill the security requirements in reputation systems. Finally in section 4 we describe an example for an implementation of a system following the concept of multilateral security by and in reputation systems.

2 Multilateral security by reputation systems

When interacting with others users necessarily have several security requirements. Interactions between interaction partners usually consist of several actions depending on each other. On the Internet these actions are usually transmitted as distinct messages. For a single message security requirements of its sender and recipient(s) are well studied. But the dependency of several messages and the meaning of the messages as actions introduces new security requirements as we will outline in this section.

2.1 Security requirements for communication

For pure communication security requirements have been studied in [25]. One should differentiate between the content of the communication and the circumstances under which it is made. Clearly, the sender and the recipient are circumstances of the communication, however there might be further circumstances

[3] `http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=orms` (last visited Jan. 09)

[4] Privacy and Identity Management for Europe (`http://www.prime-project.eu/` (last visited Jan. 09)), funded by the European Union in the 6. Framework Program, 2004-2008.

senders and recipients want to protect, e.g., the time of communication or the location they are in when communicating with each other. Based on this, security requirements are structured as in Table 1.

protection of / threats	content	circumstances
unauthorised access to information	confidentiality hiding	anonymity unobservability
unauthorised modification of information	integrity	accountability
unauthorised impairment of functionality	availability	reachability legal enforceability

Table 1. Security requirements for communication [25]

The requirements are defined as follows:

- *Confidentiality* ensures the confidentiality of user data when they are transferred.
- *Hiding* ensures the confidentiality of the transfer of confidential user data.
- *Anonymity* ensures that a user can use a resource or service without disclosing his identity.
- *Unobservability* ensures that a user can use a resource or service without others being able to observe that the resource or service is being used.
- *Integrity* ensures that modifications of communicated content (including the senders name, if one is provided) are detected by the recipient(s).
- *Accountability* ensures that sender and recipients of information cannot successfully deny having sent or received the information.
- *Availability* ensures that communicated messages are available when the user wants to use them.
- *Reachability* ensures that a peer entity (user, machine, etc.) either can or cannot be contacted depending on user interests.
- *Legal enforceability* ensures that a user can be held liable to fulfill his legal responsibilities within a reasonable period of time.

2.2 Fulfilment of semantic security requirements

Interaction partners necessarily have security requirements in common concerning the content of the message transferred. These requirements can be fulfilled by technical measures only to the extent the interaction partners cooperate and behave as expected. This means, interaction partners typically have an expectation regarding the behaviour of the interaction partners that these might fulfil or not. Fulfilment of expectation might be defined implicitly (e.g., behaviour follows social norms) or even explicitly (e.g., on the basis of a contractual agreement). In an interaction system this means:

– Technical confidentiality might become useless for a user if interaction partners redistribute the content of confidential messages.
– Technical integrity might become useless if the one who wrote an message with integrity gives a false or useless statement by the message.
– Technical availability of an interaction system might become useless for a user if none is willing to interact.

For this reason the security requirements regarding the content of the message have to be reformulated in comparison to [25] as already outlined similarly in [1]:

– *Confidentiality* does not only address the confidentiality of data transferred in an action, but also *discretion* of the interaction partner regarding the data he received and may forward to third parties.
– *Integrity* does not only address that modifications of communicated content (including the senders name if one is provided) are detected by the recipient(s), but also that the recipient is able to decide on the *bona fides* of the action performed by the message, i.e. that he is able to decide on it.
– *Availability* does not only address that resources are available when the user wants to use them, but also the *willingness* of others to interact.

By these definitions security requirements have an explicit part addressing the technical system and an implicit part addressing the semantic fulfilment of the requirement by the (possible) interaction partner(s). It is difficult to judge on the implicit part of security requirements in an objective way. Willingness usually can be judged on in an objective way because it is easy to see whether users participate in interactions or not. Bona fides usually are subjective. Breakage of discretion often might not become known directly.

Although numerous cryptographic primitives and building blocks help to fulfil requirements of interactions on the explicit technical level, interaction partners still have numerous possibilities for misbehaviour regarding the implicit requirements. Legal enforceability helps to ensure an interaction partner behaving as agreed beforehand. But many interactions between individuals might be more informal, or it might be too expensive to enforce liability.

Reputation systems have been established to collect experiences about users' behaviour in interactions and thereby they collect the fulfilment of implicit forms of security requirements. Currently reputation systems (e.g., the one eBay uses) are mainly used to collect information about users' bona fides but also information on users' willingness and discretion could be collected.

2.3 Linkability of actions and resulting security requirements

An interaction usually consists of numerous individual but correlated actions. Correlating actions lead to new security requirements:

The *unlinkability* of two or more items of interest (e.g., of actions) from the attackers perspective means that within the system (comprising these and

possibly other items), the attacker cannot sufficiently distinguish whether these items of interest are related or not [15].

The linkability of actions transmitted by messages has an effect on the security requirements formulated for single messages. Particularly in terms of anonymity, the linkability of actions can reveal identities. In the case of pseudonyms, it is at least possible to link actions performed under the same pseudonym. This is exactly what pseudonyms are used for. With respect to security requirements and as security requirement itself, *pseudonymity* can have various flavors, e.g., the unlinkability of actions performed under different pseudonyms, and the unlinkability of the pseudonym to the holder (i.e., holder anonymity) with the possible exception of specific pre-defined conditions to reveal information about the holder [15].

Further, the *absolute linkability* of actions could have positive effects on fulfilling integrity and availability requirements and, therefore, could be desirable [25]. In particular, it allows additional security requirements to be applied to a set of actions or messages: *Authorisability* of a pseudonym ensures that a pseudonym can be authorised to perform a certain action after it has authenticated itself with another action.

2.4 Multilateral security

In interactions often security requirements are contradicting. Here multilateral security means providing security for all parties involved, requiring each party to only minimally trust in the honesty of others [19]:

- Each party has its particular security requirements.
- Each party can formulate its security requirements.
- Conflicts between security requirements can be recognised and compromises negotiated.
- Each party can enforce its security requirements within the agreed compromise.

2.5 Identity management

Identity management systems (IMS) both try to help users to manage the various digital identities and the corresponding user accounts they establish with Internet applications and/or help application providers to manage the users registered with them. Depending on the application and the situational context a user is in, he decides which user account to create or to use. Many applications require users to declare at least some (often reliable, e.g., by external authentication) personal data when creating a user account. However, users often want to stay as anonymous as possible as long as it is not necessary to disclose data to get certain services. The use of a user account and the often corresponding consecutive disclosure of personal data (beginning with just surfing through shops to order certain products) have to be supported by IMS which assist the user in the explicit (and hopefully also implicit) disclosure of personal data.

This requires privacy-enhancing IMS (PE-IMS) to support and integrate techniques of multilateral security in order to achieve especially the following two of the security requirements outlined above [6]:

- *Pseudonymity controlled by the user* consists of two aspects: Unlinkability of a user account to its holder (called holder anonymity): Other parties do not know, which holder the user account is linked to. Unlinkability of user accounts: Other parties do not know, whether or not different user accounts are of the same user.
- *Accountability of a user controlled by others:* A pseudonym can be authenticated in a secure way and, based on this, be authorised to use specific services. When necessary (e.g., in the sense of legal enforceability), the holder of the pseudonym can be held liable for actions performed under this pseudonym.

3 Multilateral security in reputation systems

A reputation network is a social network that links entities (possibly pseudonymously) to each other and allows them to interact and exchange information with each other. On the one hand entities within the reputation network can learn possible interaction partners' reputation from former interaction partners or other entities within the network who observed the possible interaction partner. In social sciences this is called the **learning mechanism** of the reputation network [2]. On the other hand entities within the reputation network may control others in the reputation network by spreading information about the entities' former interactions. In social sciences this is called the **control mechanism** of the reputation network [2].

Both entities and interactions within the reputation network can be reputation objects. Entities and non-completed interactions are *dynamic reputation objects* while completed interactions are *static reputation objects*. Reputation systems assist reputation networks technically. We assume that they collect explicit reputation only about members who agreed on collecting it because according to [3] opinions about a natural person can be seen as personal data the respective person's right on informational self-determination should be applied to. For this reason a reputation system has to assist explicit membership actions regarding a reputation network resp. system. A person must be able to apply for membership under a certain pseudonym in a reputation network and also must be able to terminate his membership.

For interactions within the reputation network we assume different interaction systems to be in place (e.g., simple e-mail, file sharing, community systems).

To implement both learning and control mechanism of the reputation network a reputation system has to offer the following actions to the members:

- **Learning mechanism through evaluation of reputation:** All members that influence the reputation of an object by their ratings, additional trusted third parties, the reputation object itself and possible future interaction

partners might evaluate a reputation's object following specific rules that are fixed by the designer of the reputation system. Every evaluator might receive a different reputation of the reputation object.
The selection of ratings used for the evaluation depends on both the information flow of ratings in the reputation network and the trust structure on the reputation network, i.e. how evaluators trust in ratings from other members. Those who rate need to be trusted in giving a correct rating which is in line with their view on a specific interaction.
- **Control mechanism through rating:** There are two types of members who can make use of the control mechanism, the interaction partner in the form of interaction-derived reputation and possible observers in form of observed reputation [17]. The system provides authorised raters with a rating function that allows them to map reputation objects to ratings. The reputation system updates the reputation of the reputation object from the ratings received.

After the creation of reputation it has to be stored somewhere. Reputation might be stored

- *centralised* at reputation servers designated for this purpose.
- *locally* at the device of the user whose pseudonym received the reputation
- *distributed* at the devices of other users.

The reputation selection for evaluation can be:

- *global:* This means the information flow within the reputation network is complete and every evaluator gets the same reputation of a reputation object.
- *individual:* This means an evaluator only gets a partial view on the reputation available.

In [24] a simpler categorisation in four classes is made that merges the aspects of storage and data flow but we found it advisable to separate these aspects.

As outlined above there are five components of a reputation system:

- **rating algorithm** of a rater,
- **reputation algorithm** for reputation update,
- **propagation of reputation and ratings** for reputation selection,
- **storage of ratings and reputation**, and
- **evaluation of a reputation object's reputation** by the reputation evaluator.

To find design options for these components one has to consider several security requirements.

The rating and update of reputation has to follow specific rules fixed by the system designer. These rules usually depend on the application scenario and have to fulfil sociological and economic requirements. We abstract here from the concrete functions to allow a universal design interoperable with various IMS and various application scenarios. An overview over possible functions is for example given in [17]. For an economic introduction we refer to [10].

The model of a reputation system interoperable with an interaction system and a PE-IMS to enable multilateral security for the user is illustrated in Figure 1.

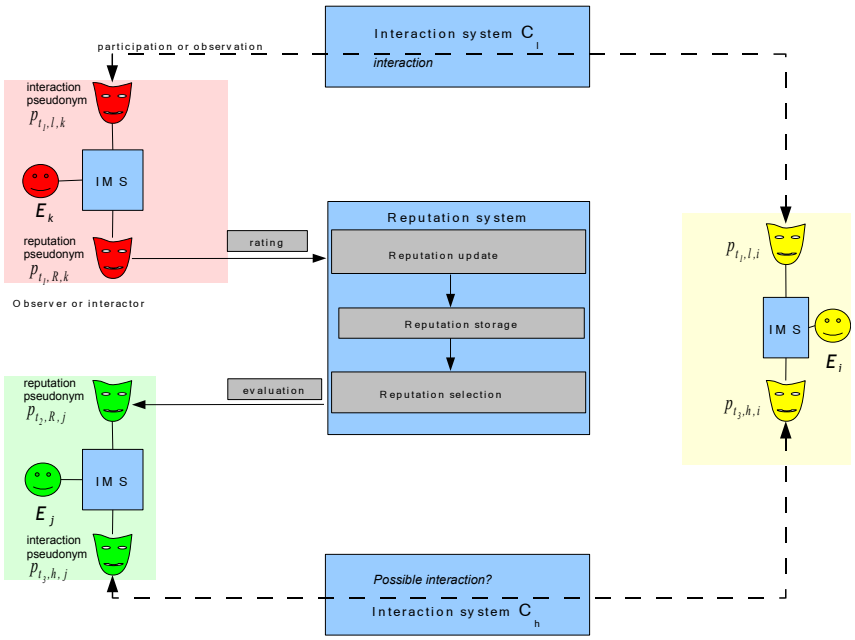

Fig. 1. System design

When a reputation system interoperates with an PE-IMS it is possible and intended that entities have several partial identities (pIDs) which cannot be linked, neither by other entities using the systems nor by the underlying system (as long as the entity does not permit this). Therefore an entity uses at least different unlinkable pseudonyms for every system he interacts in resp. with.

If there would exist only one reputation per entity, all pIDs of this entity would have the same reputation. This would ease the linking of the pIDs of one entity because of the same reputation value. Thus, having separated reputations per pID and not only one per entity is a fundamental condition for a reputation system in the context of identity management.

The use of pIDs brings forward the problem that a malicious entity may rate himself a lot of times using new self created pID for every rating in order to improve his own reputation. This kind of attack is also known as Sybil attack [12]. If the reputation system is not defined carefully it would be easy for such an attacker to improve the own reputation unwarranted. This can be limited/prevented by entrance fees or the use of once-in-a-lifetime credentials as suggested in [14].

3.1 Multilateral security

Beneath the security requirements for communication based on the functional requirements of the learning and control mechanism of the reputation network new security requirements for reputation systems can be identified:

- *Bona fides of ratings and reputation:* If it would be possible for all members of a reputation network to observe an interaction and if all of them would give the interaction the same rating this rating would have *objective bona fides*. But most ratings depend on subjective estimation of the interaction partners or observers at a certain point in time. As a special action a rating has *subjective bona fides* for an observer if it corresponds to his expectation of the interaction. Accordingly a reputation has subjective bona fides if it is created by bona fides from ratings done by bona fides.
- *Fairness of the underlying game-theoretic trust game:* A reputation system is fair if every authorised entity has the same possibilities for rating an interaction partner. The authorisability in the reputation system has to follow the control mechanism of the reputation network. Only entities that gave a leap of faith to interaction partners should be able to rate them.
- *Completeness of reputation:* Members of a reputation network expect to receive as much information as possible from interactions performed in the reputation network. This needs the willingness of authorised interaction partners to rate each other and the willingness of all members to distribute reputation in the reputation network.
- *Persistence of reputation objects:* To help the control mechanism to be employed longevity resp. persistence [20] of members as reputation objects has to be realised resp. the binding of reputation to them. This can be done pseudonymously.
- *Absolute linkability of a user's membership in a reputation network:* To prevent a user from leaving a reputation network with a bad reputation and re-entering it with a neutral reputation membership actions of the same user in the same context have to be absolutely linkable.

By actions in the reputation network no other requirements on interactions should be affected. This needs unlinkability of actions and pseudonyms of the same user in different interaction systems and the reputation network as well as providing anonymity to him.

The following building blocks are able to reach a compromise between the users' wish for completeness of reputation and the unlinkability and anonymity of his actions in the sense of multilateral security:

Parallel usage of pseudonyms: *Unlinkability of a user's actions in different contexts* can be reached by context-specific pseudonyms [23]. This enables users to collect reputation in different contexts separately. Hopefully this should also increase the *objective bona fides of reputation* because users usually behave different in different contexts and also have different expectations in different contexts.

Convertible credentials between interaction and reputation system: The rater's actions in interaction system and reputation system can be unlinkable. This needs a Third Party to be in place that issues a convertible credential [5] to an interaction pseudonym that the respective user can convert to his reputation pseudonym and that allows him to give a rating to an interaction partner specified in the credential. This enables *fairness of the interaction's trust game*. Both *pseudonyms are unlinkable* to each other for everyone but himself. Certainly he can only be *anonymous* in the set of other users who might be allowed to give a rating to the same pseudonym.

Pseudonym change with reputation transfer: If members want to limit the pseudonymous profile that can be built for them based on the interactions they were involved in they have to change their pseudonym from time to time in the form that the old pseudonym gets invalid and a new one with the same reputation gets valid. The same reputation is needed to ensure *persistence of reputation objects* and *completeness of reputation*. According to [22, 23] this can be realised by convertible credentials. A pseudonym change with reputation transfer only makes sense if there are enough other users with the same reputation who also change their pseudonyms. These users form the anonymity set for the pseudonym change.

Limitation of the rating and reputation set: The size of the anonymity set possible for a pseudonym change depends also on the reputation set and the visibility of raters and ratings in a user's reputation. Both reputation and rating set should be chosen small enough to enable sufficiently large anonymity sets.

4 System

To show how the building blocks can be composed to a multilateral secure reputation system in a multilateral secure environment we implemented a system design as outlined in [18]. We decided to use a centralised implementation of an interaction system as test bed for interactions between users. In a centralised system interactions between members take place via a central server where they are stored and globally available. Thereby a virtual community [21] is created. To become a member of the community a user has to register with the community server by declaring a pseudonym for use within the community. We chose the web forum software phpBB[5] for our implementation.

The reputation system we implemented uses global reputations that are stored at the users' device to give him control over personal data including his reputation. Our design is independent from concrete rating and reputation algorithms.

We assume all communication to be secured by encryption to reach confidentiality of all ratings and actions performed. All actions and ratings have to be secured by digital signatures given under a pseudonym for integrity reasons. By the use of an identity provider accountability of the pseudonym can be given.

[5] `http://www.phpbb.com/` (last visited Jan. 09)

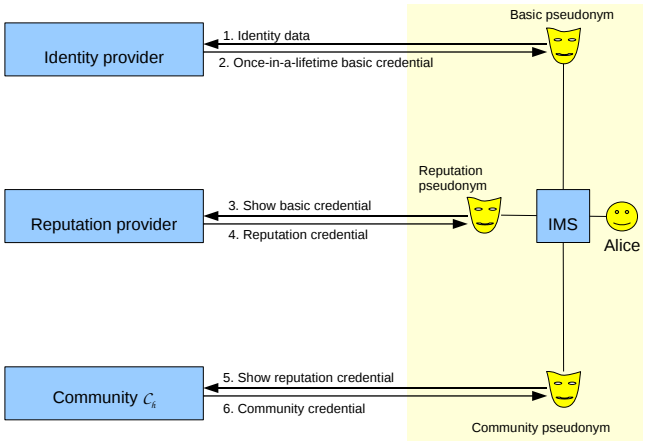

Fig. 2. Registration process enabling unlinkability of a user and his pseudonyms

For the identity management a user Alice registers a basic pseudonym with an identity provider by declaration of her identity data (step 1 in Fig. 2). After verifying the data the identity provider issues a basic credential (step 2 in Fig. 2).

When Alice wants to register in a reputation network within a certain context she sends the reputation provider her basic credential (step 3 in Fig. 2). This guarantees no user is able to build up reputation under multiple pseudonyms within the same context and every user can be identified in the case of misbehaviour. The reputation provider creates a reputation pseudonym based on the basic pseudonym and sends it back to Alice (step 4 in Fig. 2).

The reputation credential contains the pseudonym and its initial reputation. The credential is a pseudonymous convertible credential the user can convert to another pseudonym within the reputation network whenever he wants to reach unlinkability of actions. The credential also contains an attribute for the context, a number of attributes for the number of last ratings to be stored and an attribute for the expiration date.

After the conversion of the reputation credential to a community pseudonym Alice can register this pseudonym with a community $\mathcal{C}_h$ by showing the converted credential (step 5 in Fig. 2). Thereby she agrees that she will collect reputation for her interactions in the community with the reputation network she registered with. Based on this she gets a community credential to her community pseudonym and becomes a member of the community (step 6 in Fig. 2).

By the use of these distinct pseudonyms, unlinkability of the actions performed under these pseudonyms is given initially. The only exception are Alice's reputation pseudonym and community pseudonym because Bob wants to assure that he actually gave the rating to the pseudonym he interacted with.

4.1 Design

In the following we outline the design of our reputation system.

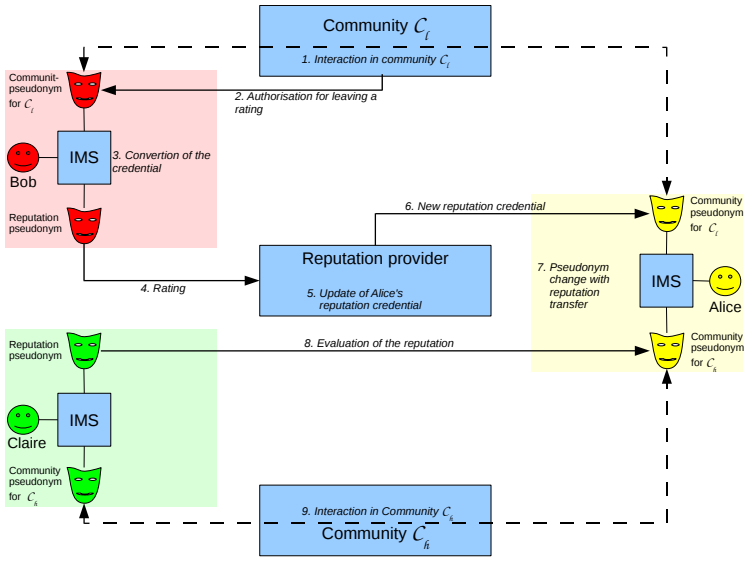

Fig. 3. System design

After an interaction (step 1 in Fig. 3) between pseudonyms of Alice and Bob Bob receives a convertible credential from the community that states that an interaction has been finished and Bob is allowed to rate Alice's pseudonym (step 2 in Fig. 3). Bob is able to convert this credential from his community pseudonym to his reputation pseudonym (step 3 in Fig. 3).

For the rating (step 3 in Fig. 3) Bob sends this credential, Alice's pseudonym and the actual rating he wants to give to Alice to the reputation provider who tests its validity and stores the rating until the update of Alice's reputation.

After a fixed number $k \geq 1$ of ratings have been given to Alice's pseudonym its reputation has to be updated by the reputation provider (step 5 in Fig. 3). We do not fix $k = 1$ here because according to the game-theoretical analysis in [11] it might make sense economically not to update a reputation after every rating but only after $k > 1$ ratings. This also increases Alice's unlinkability.

For the update Alice has to send her reputation credential to the reputation system. This might be either initiated by Alice or by the reputation provider. The attribute containing the reputation has to be updated in the reputation credential and the new rating has to be added as attribute to resp. substitute of one of the existing expired rating attributes. The reputation provider does not need to know the reputation value. Only the relationship between the old and the new credential must be guaranteed by the reputation provider. Therefore

in principal the calculation is possible on encrypted values if the reputation computation algorithm is homomorphic regarding the encryption.

The reputation computation algorithm can be chosen arbitrarily by paying attention to the fact that users are recognisable by their reputation even if they use convertible credentials to reach unlinkability of their actions. For this reason the sets of possible reputations and ratings have to be small enough to reach large enough anonymity sets. Details about this idea are outlined in [23].

For the update the reputation provider sends the new reputation credential to Alice (step 6 in Fig. 3). The old reputation credential would still be valid if it did not contain the attribute for the expiration date.

To increase the unlinkability between different interactions of a user, the change of pseudonyms with reputation transfer is possible as suggested in [23] (step 7 in Fig. 3). This is realised by pseudonymous convertible credentials that allow a user to maintain his reputation but use a new pseudonym without trusting the reputation provider.

A pseudonym change only makes sense when a large number of users with the same attributes (here the same reputation if no other attributes are known) changes their pseudonym at the same time to guarantee an appropriate anonymity set. For this reason the sets of possible rating and reputation values are limited.

If Alice wants to change her pseudonym while a rating has been left at the reputation provider for her credential, it cannot be guaranteed that the mapping between the new pseudonym and the rating could be made. Therefore the reputation provider has to authorise the pseudonym change indirectly by issuing credentials with new expiration dates. By this he helps to collect an anonymity set of users willing to change their pseudonyms.

Before deciding on an interaction with a member of the community $\mathcal{C}_h$ Claire can evaluate pseudonymously its reputation after the member send her the reputation credential (step 8 in Fig. 3).

To augment the availability of the reputation a storage at the reputation server or the community server should be possible with the chance for the user to appoint authorisation to other members of the community to see the reputation.

Alice can always leave the community or reputation network. If she then has a reputation less than the initial reputation her identity should be revealed to all identity providers cooperating with the respective reputation provider and community system. They will ban Alice for further registration to guarantee that she does not get any new basic pseudonyms she could use for a new registration in the reputation network or a community. This implements the once-in-a-lifetime-credentials introduced in [14].

4.2 Implementation

phpBB The software phpBB was originally developed as software for forums. Therefore text-based interactions can be carried out with the help of phpBB. The framework has a centralised architecture that must be installed on a web server using PHP as script language. It supports various database schemes (MySQL, etc.). The user uses the system only with the help of a web-based interface. The

basic phpBB implementation allows users to register with the community, to start and answer a thread. For a reputation system like ours where users should be rated based on interactions it is crucial that a mechanism exists, which proves that the interaction has actually happened and was finalised. Such a mechanism provides the MOD "Geocator's Feedback Ratings MOD"[6]. Besides it includes a whole reputation system in an eBay-like style we do not make use of.

Reputation system The credentials and the required functions for handling them were implemented using the idemix-Framework[7], which is written in Java.

The reputation system is independent from the community server but can be called over links integrated in the phpBB framework. These links lead to PHP-based websites, offering different functions of the reputation system.

The websites request the users to fill in the necessary specifications like the reputation credential or the rating value. If the inputs are valid after checking by the reputation system, the PHP-scripts call a Java program implementing the respective reputation functions. The programs are either dealing on the credentials (e.g. the update function) or on one of the databases also implemented by the idemix framework (e.g. the rating function, where the rating remains in the database till the reputation object updates his reputation credential). Also the published reputation is in one of these databases. Functions to remove one's reputation and to search for other members' reputation are also existent.

Fig. 4. Extended interface of phpBB

The prototype does not use PRIME yet but uses the authentication methods of phpBB. Therefore the registration process takes place simultaneously in the phpBB community and the reputation system. The phpBB community could be used as usual, but the member can call the reputation functions within the phpBB interface that have been extended for this reason as illustrated in Fig. 4.

Pseudonym change The pseudonym change is implemented in an Java-program which can be executed on the user's system without knowledge of the reputation provider, the community or other members.

[6] `http://www.phpbb.com/community/viewtopic.php?f=16&t=381862` (last visited Jan. 09)

[7] `http://www.zurich.ibm.com/security/idemix/` (last visited Jan. 09)

5 Conclusion

The basis and preconditions to design reputation systems in a multilateral secure way were introduced. This concept becomes more and more important with the growing number of applications which need reputation systems.

Our current research concentrates on different forms of interactions systems and the interoperability arising between them. Here our focus lies on authentication methods using a PE-IMS like PRIME.

For the future is planned to develop distributed alternatives to the central reputation providers. This will hopefully allow for individual reputation additionally to the global reputation in our current system design.

6 Thanks and disclaimer

I would like to thank Vacláv (Vashek) Matyáš and Simone Fischer-Hübner for their invitation to write this paper for the FIDIS summerschool proceedings. The research described in section 4 was partially done with Franziska Pingel whom I want to thank for this. I also thank Marc van Lieshout for his helpful review of this paper.

The research leading to the results presented in this paper has received funding from the European Communitys Sixth and Seventh Framework Programme (FP6/2002-2006 resp. FP7/2007-2013) for the projects FIDIS, PRIME and PrimeLife. The information in this document is provided as is, and no guarantee or warranty is given that the information is fit for any particular purpose. The consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

References

1. Katrin Borcea-Pfitzmann, Marit Hansen, Katja Liesebach, Andreas Pfitzmann, and Sandra Steinbrecher. Managing one's identities in organisational and social settings. *DuD, Datenschutz und Datensicherheit*, 31(9):671–675, 2007.
2. Vincent Buskens and Werner Raub. Embedded trust: Control and learning. In Ed Lawler and Shane Thye, editors, *Group Cohesion, Trust, and Solidarity*, volume 19 of *Advances in Group Processes*, pages 167–202, 2001.
3. L. Bygrave. *Data Protection Law, Approaching Its Rationale, Logic and Limits.* Kluwer Law International, The Hague, London, New York, 2002.
4. C. Camerer and K. Weigelt. Experimental tests of a sequential equilibrium reputation model. *Econometrica*, 56:1–36, 1988.
5. David Chaum. Showing credentials without identification. Signatures transferred between unconditionally unlinkable pseudonyms. In *Advances in Cryptology - EUROCRYPT '85, Workshop on the Theory and Application of of Cryptographic Techniques*, pages 241–244, New York, NY, USA, 1986. Springer-Verlag.

6. Sebastian Clauß, Dogan Kesdogan, Tobias Kölsch, Lexi Pimenidis, Stefan Schiffner, and Sandra Steinbrecher. Privacy enhancing identity management: Protection against re-identification and profiling. In Atsuhiro Goto, editor, *DIM '05, Proceedings of the 2005 ACM Workshop on Digital Identity Management*, pages 84–93, Fairfax, Virgina, USA, November 2005. ACM.
7. Sebastian Clauß and Marit Köhntopp. Identity management and its support of multilateral security. *Computer Networks*, 37(2):205–219, October 2001.
8. Sebastian Clauß , Andreas Pfitzmann, Marit Hansen, and Els Van Herreweghen. Privacy-enhancing identity management. *The IPTS Report*, 67:8–16, September 2002.
9. Partha Dasgupta. Trust as a commodity. In Diego Gambetta, editor, *Trust: Making and Breaking Cooperative Relations*, pages 49–72. Department of Sociology, University Oxford, 2000.
10. Chrysanthos Dellarocas. The digitization of word-of-mouth: Promise and challenges of online feedback mechanisms. *Management Science*, pages 1407–1424, October 2003.
11. Chrysanthos Dellarocas. Research note – how often should reputation mechanisms update a trader's reputation profile? *Information Systems Research*, 17(3):271–285, 2006.
12. John R. Douceur. The sybil attack. In *IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems*, pages 251–260, London, UK, 2002. Springer-Verlag.
13. ENISA. Position paper. reputation-based systems: a security analysis. available from `http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_reputation_based_system.pdf` (letzter Abruf 09.02.08), 2007.
14. Eric Friedman and Paul Resnick. The social cost of cheap pseudonyms. *Journal of Economics and Management Strategy*, 10:173–199, August 1999.
15. Marit Hansen and Andreas Pfitzmann. Anonymity, unobservability, and pseudonymity - a proposal for terminology. Version 0.8 in: Hannes Federrath (Ed.): Designing Privacy Enhancing Technologies; Proc. Workshop on Design Issues in Anonymity and Unobservability, Lecture Notes in Computer Science 2009, 2001, pp. 1-9, Version 0.30 in: Rene Balzer, Stefan Kpsell, Horst Lazarek (Hg.): Fachterminologie Datenschutz und Datensicherheit Deutsch - Russisch - Englisch; FGI - Forschungsgesellschaft Informatik, Technische Universitt Wien, Wien, Februar 2008, 111-144. Version 0.31 available from `http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf`, 2007.
16. Tobias Mahler and Thomas Olsen. Reputation systems and data protection law. In *eAdoption and the Knowledge Economy: Issues, Applications, Case Studies*, pages 180–187, Amsterdam, 2004. IOS Press.
17. Lik Mui. *Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks*. PhD Thesis, Massachusetts Institute of Technology, 2003.
18. Franziska Pingel and Sandra Steinbrecher. Multilateral secure cross-community reputation systems. In S.M. Furnell S.K. Katsikas and A. Lioy, editors, *Proceedings of Trust and Privacy in Digital Business, Fifth International Conference, TrustBus*, volume 5185 of *Lecture Notes in Computer Science*, pages 69–78. Springer, 2008.
19. Kai Rannenberg, Andreas Pfitzmann, and Günter Müller. IT security and multilateral security. In Gnter Mller and Kai Rannenberg, editors, *Multilateral Security in Communications*, volume 3 (Technology, Infrastructure, Economy), pages 21–29, Mnchen, 1999. Addison-Wesley.

20. Paul Resnick, Ko Kuwabara, Richard Zeckhauser, and Eric Friedman. Reputation systems. *Communications of the ACM*, 43(12):45–48, 2000.
21. Howard Rheingold. *The Virtual Community: Homesteading on the Electronic Frontier*. Perseus Books, 1993.
22. Sandra Steinbrecher. Balancing privacy and trust in electronic marketplaces. In *Proceedings of Trust and Privacy in Digital Business, First International Conference, TrustBus*, volume 3184 of *Lecture Notes in Computer Science*, pages 70–79. Springer, 2004.
23. Sandra Steinbrecher. Design options for privacy-respecting reputation systems within centralised internet communities. In *Proceedings of IFIP Sec 2006, 21st IFIP International Information Security Conference: Security and Privacy in Dynamic Environments*, May 2006.
24. Marco Voss. Privacy preserving online reputation systems. In *International Information Security Workshops*, pages 245–260. Kluwer, 2004.
25. Gritta Wolf and Andreas Pfitzmann. Properties of protection goals and their integration into a user interface. *Computer Networks*, 32(6):685–699, 2000.