The Need for Interoperable Reputation Systems

Sandra Steinbrecher

The Need for Interoperable Reputation Systems

Sandra Steinbrecher

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

Abstract. Nowadays more and more Internet applications install reputation systems to collect opinions users have about some reputation objects. The opinions are usually formalized in the form of ratings the reputation system can use to build overall reputation profiles of the reputation objects. Reputation objects might be other users, products, web content and anything else that can be rated. Users may investigate the reputation object's reputation profile to estimate its quality resp. trustworthiness. As there are currently many providers of reputation systems it would be desirable to make reputation information in different systems interoperable or to establish meta reputation systems that collect information from various applications resp. their reputation systems. This process should consider both interoperability of reputation systems themselves and their interoperability with applications, trust and identity management systems as we will discuss in this paper.

1 Introduction

The experiences of an individual's environment influence his own interactions with others. When a friend made bad experiences with a shop the individual might become skeptical as well or even resist to buy there. The Internet offers its users the possibility to exchange knowledge and experiences regarding the online and offline world not only with others in their near environment, but with nearly everyone: Many users inform themselves about others' experiences with sellers before buying from them in a marketplace like eBay[1]. Many users inform themselves about hotels before booking a room in travel portals like tripadvisor[2]. Also many users make use of the book reviews collected in a store like amazon[3] before buying a book.

These three examples of eBay, tripadvisor and amazon have in common that the respective providers installed a reputation system that allows users to rate reputation objects of a certain category: in eBay other users, in tripadvisor objects related to traveling like hotels and restaurants, in amazon products like books the store sells.

Reputation systems can collect the experiences users make with reputation objects in a technically efficient way. These experiences may help

[1] http://www.ebay.com/ (last visited April 2010)
[2] http://www.tripadvisor.com/ (last visited April 2010)
[3] http://www.amazon.com/ (last visited April 2010)

other users to estimate the future trustworthiness resp. quality of reputation objects they have no personal experience with. But informing himself about a reputation object does not prevent any user from making bad experiences with it because e.g., reputation usually is context-dependent and subjective. Although 'social attacks' (e.g., users may lie [6] or reputation objects may change) are possible, a usually large number of ratings and an honest majority of users will hopefully achieve that dissatisfied users are the exception. So reputation systems do not make other technical security measures (like digital signatures or certifications by independent institutions) obsolete, but hopefully reduce the cases where expensive legal enforceability might become necessary.[4]

Many users do not only use one, but several reputation systems, typically they might even be reputation objects in several reputation systems. E.g., both eBay and Amazon are providers of marketplaces and many people use both. For this reason there is an interest of users in using reputation they earned in one application as reputation object also in the other application. The same holds also for the author of a book: If he got good ratings on amazon, he might want to transfer these ratings also to the reputation system of another book store that sells his book. Also the respective store is interested in getting this reputation information from another store as it will typically increase its profit to provide large reputation profiles of the products it sells.

Reputation systems are now evolving into reputation-as-service applications like epinion[5] for products or iKarma[6] for companies/individuals independent from a concrete application, but still mostly have a single-provider model. There is the vision to establish stand-alone reputation systems that collect information from various interactions and in various contexts and also to make reputation information in different systems interoperable [9]. This process should consider both interoperability of reputation systems themselves and their interoperability with various other systems as we will discuss in this paper in Sect. 3-6 after explaining the preliminaries in Sect. 2.

2 Preliminaries

For our system environment as shown in Figure 1[7], we assume applications that allow users to make experiences with a so-called reputation object. Such an application might be, e. g., a marketplace where users make experiences with sellers or a wiki where users make experiences with content and authors. Further reputation systems are provided that collect positive and negative experiences the users report to it about reputation objects in the form of ratings given with a *rating function*. The reputation system updates the reputation of the reputation object from

[4] Please note that the social and legal aspects cannot be discussed in further detail.

[5] `http://www.epinion.com` (last visited April 2010)

[6] `http://www.ikarma.com/` (last visited April 2010)

[7] Please note that we assume a user as reputation object in this Figure, but it can also be any arbitrary reputation object.

the ratings received with a *reputation function*. The reputation systems may exchange reputation between the reputation objects with the help of a *reputation exchange function*.

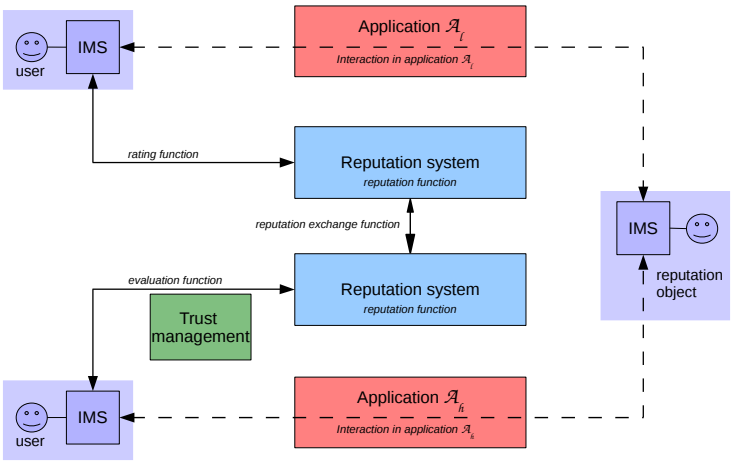

Fig. 1. System environment and arising interoperability issues

Reputation in a reputation system might be stored

- *centralized* at reputation servers designated for this purpose,
- *locally* with the reputation object itself, or
- *distributed* with other users.

If a user (the so-called evaluator) becomes interested in a reputation object, the reputation system provides him with an *evaluation function* to learn a reputation object's reputation following specific rules. The selection of ratings used by the evaluation function depends on both

- the *information flow* of ratings the system provides between the users and
- the *trust structure* between the users, i.e. how users trust in others' ratings.

The information flow is organized by the reputation system while the trust structure is determined by a trust management system that allows to assign trust values to other users. Depending on these two aspects the reputation selection for the evaluation function might 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. Here possibly every evaluator might receive a different reputation of the reputation object.

For interacting with any system users make use of an identity management system to possibly separate different partial identities they have. From this architecture four interoperability issues arise that will be outlined in the following sections. First there is the aspect of interoperability between reputation systems that will be discussed in Sect. 3. This needs interoperability of the corresponding applications to either make reputation systems interoperable or to install a common reputation system that collects ratings from several applications as will be outlined in Sect. 4. In Sect. 5 we further discuss that for the evaluation function interoperability with trust management systems should become important. Finally in Sect. 6 the possibilities for interoperability with identity management systems for the reasons of privacy and security are explained. For further issues of reputation systems' privacy and security we refer to [18, 9].

3 Interoperability of reputation systems

Typically users interact in manifold ways on the Internet. They might play, sell, post product ratings, discuss with friends on different topics and so on. As they might collect reputation in many applications, making existing reputation system(s) for these applications interoperable becomes of interest. The problem of interoperability that is represented by the reputation exchange function in our model is twofold:

- *Format:* First formats for common exchange and possibly also internal representation of reputation are needed. An OASIS group[8] works on a possible portable format using XML. But currently we still lack such a standard that could be implemented. Here is the need for solutions that can be easily integrated in the existing web technologies. The suggestion we implemented in [19] was to use the Resource Description Framework (RDF) [13] common for the Web 2.0 and allowing to add reputation information as meta-information to arbitrary web content.
- *Algorithm:* In every reputation system different implementations of rating function, evaluation function and reputation function are defined depending on the system designer. An overview of possible functions is for example given in [15]. For an economic introduction of possible advantages and disadvantages certain choices have we refer to [7]. An algorithm how to transfer reputations received from another reputation system to the own reputation system is needed. This algorithm needs to comprise inheritance rules for reputation to decide on interoperability of reputation or ratings from different reputation systems.

The OpenPrivacy Initiative[9] presented Sierra, a reference implementation of a reputation management framework comprising several components representing the functions of the reputation system as well as an identity management system. They also define reputation exchange

[8] `http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=orms` (last visited April 2010)

[9] `http://openprivacy.org/` (last visited April 2010)

functions, whose actual implementation can be determined by the system designer in terms of exchange rates between reputations calculated from different reputation functions.
However, there are other issues of interoperability between reputation systems so far neglected by the technical literature:

- *Several reputation exchanges:* For several executions of the reputation exchange functions between two reputation systems it has to be secured that it is clear which part of reputation has already been exchanged.
- *Related reputation objects:* So far we assumed that the reputation object is well determined. Another issue interoperability of reputation systems has to deal with is the possible relation between distinct reputation objects. For example a reputation system collecting reputation of content might need to exchange reputation with a reputation system collecting reputation of authors. Certainly there is some relation between a content and its authors, but it might not be advisable to transfer reputation of one content directly to its authors and vice versa. Thus reputation systems need to define the transfer of reputation between related objects by a *reputation object exchange function*.

4 Interoperability with applications

Currently the vision arises to establish stand-alone reputation systems that collect information from various interactions in different applications.
Social scientists and theoretical economists model the problem whether two users, who want to interact, should place trust in each other as a so-called trust game [2, 5] that needs inter-personal context-specific trust. The reputation system tries to assist users in this game by implementing a social network that allows users to exchange information with each other. By the evaluation function users can learn others' reputation. In social sciences this is called the **learning mechanism** of the social network [1]. On the other hand users may control other users by spreading information about the users in the social network. In social sciences this is called the **control mechanism** of the social network [1] as implemented with the rating function of the reputation system. Thus, he applications, where the interactions rated took place, have to provide the reputation system with as much information as possible on the following aspects:

- *Model of Trust Game:* Only users, who gave a leap of faith to reputation objects should be able to rate them. Applications have to make a clear model, who gave a leap of faith and specify this for the reputation system.
- *Interaction information:* As reputation is context-dependent information on the interaction rated is needed, e.g., time, value for the interaction partners.
- *Rater information:* As reputation needs to build on inter-personal trust also information on the raters is needed as will be outlined in Sect. 5

Beneath the OpenPrivacy Initiative mentioned in Sect. 3 there are commercial stand-alone systems like iKarma as 'third-party service for collecting, managing and promoting [your] reputation among [your] customers and contacts.'[10] or portals like Trivago[11] that comprises reputation information from various other reputation systems.
The scientific approaches, that outline reputation infrastructures independent from concrete applications (e.g., [20, 16, 11, 17], do not follow the centralised approach of the commercial solutions, but use local storage of reputation information to enable users to show the reputation they collected to others themselves. All of these suggestions need some external infrastructure to prevent reputation manipulation by the reputation object.
In the mentioned scientific approaches the trust model is implicitly clear, but as all of them aim for a privacy-respecting reputation system neither interaction nor rater information is provided. For the commercial solutions users can provide as much information as they want on themselves and their interactions.

5 Interoperability with trust management

As outlined in Sect. 2 reputation networks need to have some kind of inherent trust structure. When a user wants to determine a reputation object's credibility resp. trustworthiness he has to determine his trust in two other sources as well:

- *Raters:* The ratings given by raters can be:
  - *subjective ratings*, that are influenced by the raters' subjective estimation of the reputation object, or
  - *objective ratings*, that can be verified by all other users than the rater at some point in time and that would have come to the same ratings.

  An example for the first type of ratings is eBay while examples for the second type can be found in P2P systems, e.g. GNUnet[12], where the reply to a query leads to a positive reputation, and a reply can be proved or verified at least at the time it is sent.
  If the raters are humans as in our model from Sect. 2, subjective ratings will be given. Then the rater needs to decide whether he would have come to the same rating; this means their views on the reputation object is interoperable. For this reason a trust management system to determine the inter-personal trust in raters is needed. It can be realized by an additional reputation system for raters.
- *Reputation systems:* Evaluators need to have system trust in all reputation systems that collected the ratings and calculated the reputation the user evaluates.

Technically trust management is often associated with PKI structures [14] (beneath other approaches). PKI structures allow to bind keys to

[10] `http://ikarma.com/support/faq/#1` (last visited April 2010)
[11] `http://www.trivago.com/` (last visited April 2010)
[12] `www.gnunet.org` (last visited April 2010)

pseudonyms. Others can use their key to sign this binding. Thereby chains to other users, who want to trust in this binding can be built. These chains can be done hierarchically with certification authorities or in the form of the web of trust (e.g., GPG/PGP). Both structures could and should also be used for the broader deployment of reputation systems. Hierarchies and chains as they work for trust management could be applied to reputation management to express which experiences from others can be trusted.
However, the straightforward approach to implement ratings as signatures and use existing PKI structures only assures accountability of keys and linkage to their holder. But if a user or certification authority signs someone's key in a PKI structure that does not say anything about the credibility/ competence they assume the key holders to have as reputation objects. For this reason different key(s) than for accountability are needed and eexisting certificate structures have to be extended appropriately.

6 Interoperability with identity management

For the evaluation function of reputation systems not only the overall reputation, but also the single ratings and the raters, who gave them might be important. If raters misbehave maliciously by giving ratings, that do not reflect the concrete experience they made with reputation objects, there should be a possibility to detect this and probably to make them accountable for that.
But for the collection of large reputation profiles about users (both reputation objects and raters) privacy also 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 [12].
For managing this a reputation system should be interoperable with privacy-enhancing user-controlled identity management systems (PE-IMS). An IMS in general is able to certify users and grant rights to them for applications. Additionally a PE-IMS [3, 4] like PRIME[13] assist 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.
The interoperability of a reputation system with a PE-IMS needs a privacy-respecting design of reputation systems while keeping the level of trust provided by the use of reputations as outlined in [18].
When a reputation system interoperates with a PE-IMS it is possible and intended that users have several partial identities (pIDs) which cannot be linked, neither by other users using the systems nor by the underlying system (as long as the user does not permit this). Both raters and reputation objects might only be known by pseudonyms to each other.

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

If there would exist only one reputation per user, all pIDs of this user would have the same reputation. This would ease the linking of the pIDs of one user because of the same reputation value. Thus, having separated reputations per pID and not only one per user is a fundamental condition for a reputation system in the context of identity management.
The use of pIDs arises the problem that a malicious user 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 [8]. 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 [10]. When using PRIME as IMS the latter can be implemented by its identity provider issuing such credentials. Alternatively or additionally also fees could be collected.

7 Resulting infrastructure

For users as reputation objects we outline in the following a possibly resulting secure reputation system interoperable with an application, an identity and trust management. Our design description is independent from concrete rating, reputation and evaluation functions.
We assume all communication to be secured by encryption to reach confidentiality of all ratings and actions performed. Also all messages should be transferred in an anonymous way with an anonymous communication network. All actions and ratings have to be secured by digital signatures (given under a pseudonym) for integrity reasons.
For the identity management a user registers himself with an identity management system (provider) by declaration of his identity data (step 1 in Fig. 2). After verifying the data the identity provider issues a credential or certification on (part of) these data (step 2 in Fig. 2). By the use of an identity management system (provider) accountability of the pseudonym can be given.
When the user wants to register with a reputation system (provider) he sends it the certification/credential he got from the identity management system (provider) (step 3 in Fig. 2). This should guarantee that 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 misbehavior. The reputation system (provider) creates a reputation certificate/credential based on the certificate/credential from the identity management system (provider) and sends it back to the user (step 4 in Fig. 2).
The reputation credential contains the user's reputation pseudonym, its initial reputation and possibly other attributes like the applications it can be used in or an expiration date.
Based on the reputation credential the user can register himself with an application by showing his reputation certificate/credential (step 5 in Fig. 2). Thereby he agrees that he will collect reputation for his interactions within the application (e.g., a marketplace or a wiki) with the reputation system he registered with. Based on this he gets an application credential to use the application (step 6 in Fig. 2).

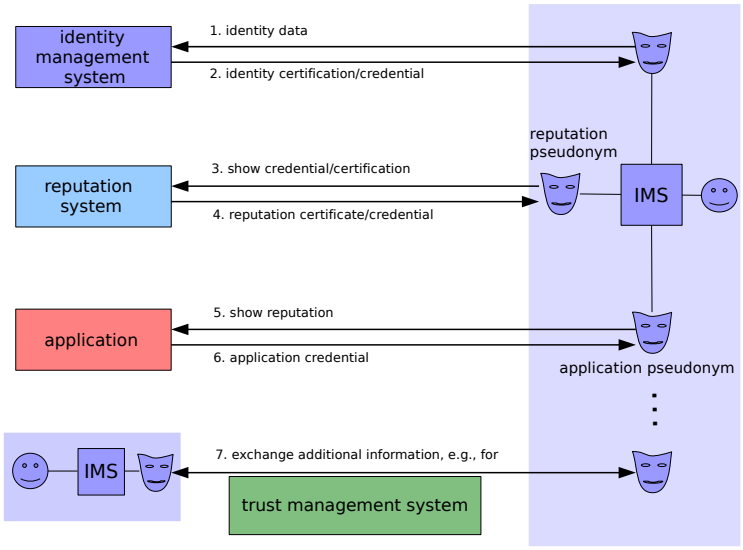

Fig. 2. Infrastructure for users as reputation objects

Additionally the user might interact with other users to exchange additional information, e.g. via a trust management system to inform himself about this user (possibly as a rater) and other users in the reputation network (step 7 in Fig. 2).

Every action the user performs above can be done under distinct pseudonyms if convertible credentials are issued by the respective providers. We implemented this infrastructure for phpBB as application and the user-controlled privacy-enhancing identity management PRIME as outlined in [16]. Currently we lack a trust management in our implementation.

8 Conclusion

In this paper we gave a first impression which aspects of interoperability should be considered for reputation systems. We also described a possible infrastructure for interoperability between applications, reputation, trust and identity management systems from a technical perspective. For interoperability of reputation systems themselves and implementing corresponding rating, reputation and evaluation functions an overall treatment from various scientific disciplines will be needed to come to suitable solutions usable in practice.

9 Acknowledgements

The research leading to these results has received funding from the European Communitys Seventh Framework Programme (FP7/2007-2013) for the project 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 PrimeLife 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.
For comments on preliminary versions of this papers I would like to thank the anonymous reviewers. Additionally Stephan Groß and Vashek Matyas provided valuable comments.

References

1. 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.
2. C. Camerer and K. Weigelt. Experimental tests of a sequential equilibrium reputation model. *Econometrica*, 56:1–36, 1988.
3. Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, and Els Van Herreweghen. Privacy-enhancing identity management. *The IPTS Report*, 67:8–16, September 2002.
4. Sebastian Clauß and Marit Köhntopp. Identity management and its support of multilateral security. *Computer Networks*, 37(2):205–219, October 2001.
5. 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.
6. Chrysanthos Dellarocas. Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior. In *EC '00: Proceedings of the 2nd ACM conference on Electronic commerce*, pages 150–157, New York, NY, USA, 2000. ACM Press.
7. Chrysanthos Dellarocas. The digitization of word-of-mouth: Promise and challenges of online feedback mechanisms. *Management Science*, pages 1407–1424, October 2003.
8. 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.
9. 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.
10. Eric Friedman and Paul Resnick. The social cost of cheap pseudonyms. *Journal of Economics and Management Strategy*, 10:173–199, August 1999.

11. Sandeep S. Kumar and Paul Koster. Portable reputation: Proving ownership across portals. In *Proc. of the European Context Awareness and Trust 2009 (EuroCAT09), 3rd Workshop on Combining Context with Trust, Security, and Privacy*, volume 504, pages 21–30. CEUR Workshop Proceedings, September 2009.
12. 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.
13. Frank Manola and Eric Miller. RDF Primer. W3C Recommendation, W3C, February 2004. available from `http://www.w3.org/TR/rdf-primer/` (last visited 07/01/09).
14. Ueli Maurer. Modelling a public-key infrastructure. In E. Bertino, editor, *European Symposium on Research in Computer Security — ESORICS '96*, volume 1146 of *Lecture Notes in Computer Science*, pages 325–350. Springer-Verlag, September 1996.
15. Lik Mui. *Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks*. PhD Thesis, Massachusetts Institute of Technology, 2003.
16. 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.
17. Stefan Schiffner, Sebastian Clauß, and Sandra Steinbrecher. Privacy and liveliness for reputation systems. In *Proceedings of 2009 European PKI Workshop (EuroPKI'09)*. Springer, 2010. (to appear).
18. Sandra Steinbrecher. Enhancing multilateral security in and by reputation systems. In *Proceedings of the IFIP/FIDIS Internet Security and Privacy Summer School, Masaryk University Brno, 1-7 September 2008*, volume 298 of *IFIP AICT*, pages 135–150. Springer, 2009.
19. Sandra Steinbrecher, Stephan Groß, and Markus Meichau. Jason: A scalable reputation system for the semantic web. In *Proceedings of IFIP Sec 2009, IFIP International Information Security Conference: Emerging Challenges for Security, Privacy and Trust*, volume 297 of *IFIP AICT*, pages 421–431. Springer, May 2009.
20. Marco Voss. Privacy preserving online reputation systems. In *International Information Security Workshops*, pages 245–260. Kluwer, 2004.