A Multidimensional Reputation Scheme for Identity Federations*

Isaac Agudo and Carmen Fernandez-Gago and Javier Lopez
Network, Information and Computer Security Lab
www.nics.uma.es
{isaac,mcgago,jlm}@lcc.uma.es

Abstract

Deciding who to trust in the internet of services paradigm is an important and open question. How to do it in an optimal way is not always easy to determine. Trust is usually referred to a particular context, and sometimes a single user interacts in more than one given context. We are interested in investigating how a *Federated Reputation System* can help exporting trust perceptions from one context to another. We propose a model for deriving trust in online services. In this context, trust is defined as the level of confidence that the service provider holds on the subject interacting with it to behave in a proper way while using the service. Thus, we derive trust by using the reputation values that those users have gained for interacting with these services.

1 Introduction

Deciding who to trust the current internet is an important task that sometimes needs of certain techniques in order to be determined. It is easier when the interactions among users and services occur in both a physical and a virtual way.

The concept of reputation is defined by the Concise Oxford Dictionary as ‘what is generally said or believed about a person’s or thing’s character or standing’. This definition corresponds well to the view of social network researchers [33]. In fact, some efforts have been made in order to add some sociological meaning to the understanding of the reputation concept before providing a model of reputation ratings for [18].

The concept of reputation is closely linked to that of trustworthiness [16]. As mentioned in this work, the difference between trust and reputation can be easily understood by looking at these two statements:

- ‘I trust you because of your good reputation.’

*This work has been funded by MEC I+D and MICT of Spain under the research projects CRISIS (TIN2006-09242), ARES (CSP2007-00004) and by the European Commission through the research project SPIKE (FP7-ICT-2007-1-217098)

- ‘I trust you despite your bad reputation.’

These two sentences illustrate how subjective the concept of trust is, compared to the concept of reputation.

Trust is based on various factors or evidences apart from reputation, although in the absence of any other previous experience reputation is a useful mechanism for establishing trust relationships. In some systems such as for example, online communities [11, 30] the problem is twofold. First, we have to make sure that the members are who they claim to be (authentication) and then that we can trust them. Using reputation of a user in order to build trust relationships can be an interesting approach, although limited by the accuracy of the reputation system.

The issue of authentication is solved most of the times by using an Identity Management system composed of a Service Provider (SP) and an Identity Provider (IDP). The SP requests the IDP information about certain user who is registered with the IDP and is interested in accessing some service provided by the SP. Our intention is to solve the other part of the problem, that is, once a user has been authenticated by the Identity Management system we are interested in establishing whether we can trust that user. In order to achieve this we propose that the IDP maintains a reputation engine that updates and provides reputation information about users in such a way that this information can be used by the SP. By using this reputation engine users in a system can also established trust among users that will guide them in order to establish better interactions.

The paper is organized as follows. Section 2 presents some related work. Section 3 provides a classification of what we consider are the aims for improving reputation. Section 4 describes our proposal for a federated reputation system and how the reputation values can be calculated. Section 5 shows how trust can be derived within a federation by using the federated reputation system. Section 6 concludes the paper and outlines the future work.

2 Related Work

There are several reputation systems running on actual systems. Many of them are listed on the Reputations Research Network site [1]. Some are used to aid people to decide whether a seller is reliable or not; others to judge whether a book is worth reading; others are used to order news according to their relevance. Even though they use different measures for reputation all of them follow the same target: to improve the user experience.

According to Resnick [27], a working reputation system must have at least the following three properties:

1. Entities must be long lived, so that with every interaction there is always an expectation of future interactions.

2. Feedback about current interactions is captured and distributed. Such information must be visible in the future.

[1] http://databases.si.umich.edu/reputations/index.html

3. Past feedback guides buyer decisions. People must pay attention to reputations.

The third principle is focused on an e-commerce scenario, although changing buyer by user of a service provider, makes it perfectly understandable . None of these properties is exempt of difficulties. One of the main risks is the use of pseudonyms, which allows one single person having multiple online identities, making thus difficult the computation of a unique reputation value for this person.

A reputation system is more effective when there are some incentives for maintaining a good reputation level and when it is difficult to get rid of bad ratings (e.g., by creating a new account). In [16] some systems are mentioned such as Epinions, which offer a reward to members who try to maintain a good reputation; Ebay, where the reputation itself is the reward and influences future sells; or Advogato which is non profit oriented and there is no reward, it is only the ego of the members that leads them to improve their reputation.

Another important factor in a reputation system is time. Timeless reputation systems consider all reputation values as if they were gathered in the same instant, whereas time aware reputation systems will use the time instant when the reputation value was gathered in order to adjust it and modify the final reputation value. However, some authors have realised that time can influence trust. Thus, in [12] the authors mentioned that trust is a very dynamic phenomenon evolving in time and having a history. In [17] a dynamic trust model for mobile ad-hoc networks is introduced. Another trust model that takes into account past trust history of users is [3]. Herrmann [15] also considers the influence of time on trust and proposes to use cTLA (compositional Temporal Logic of Actions [14]) as a method for modelling and verifying trust mechanisms. One of the latest approaches to consider time as a parameter is that presented in [2]

As we mentioned above, there are many factors that define a reputation system. Among those factors are also the ones identified by Jeff Ubois [31]:

- **Participants**. Who is rating whom? Is the system customer-about-buyer, or peer-to-peer? Do the users that provide feedback have reputations themselves? Are they known or anonymous?

- **Incentives**. Are the participants explicitly taking part in a reputation system, or are they performing ‘normal’ tasks such as writing a newspaper article or offering advice in a Usenet group?

- **Criteria**. What issues matter to the users? Do they care about prompt shipping or about product quality? That is, what factors go into calculating a reputation: numeric feedback from counterparts to a transaction, observed behaviour, seals and credentials, press coverage, etc.?

- **Access and recourse**. Who can see the data, and who can change it? Who gets to know about that change? Who knows about who has rated whom? Can someone respond to a reputation he is assigned? Can an opinion be corroborated?

- **Presentation and tools**. Offline reputation is rich and nuanced: people can use all five senses to determine reputation. Online users can only see and interact with data points. With what tools can users interact with and filter data? To what extent is the data abstracted or aggregated?

Several research initiatives are working in the reputation field. Some of them are, for example, the Task Force on European Middleware Co-ordination and Collaboration (TF-EMC2) [29], under the auspices of the TERENA Technical Programme. Its main objective is to promote the development and deployment of open and interoperable middleware infrastructures among national and regional research and education networking organizations and academic and research institutions.

The European Network and Information Security Agency (ENISA) is also highly interested in reputation and how it could be handled in online communities. The First position paper [8] presents, as its tenth technical recommendation, the use of reputation techniques, quoting: “Encourage the Use of Reputation Techniques” The second position paper [9] aims to provide a useful introduction to security issues affecting reputation-based systems by identifying a number of possible threats and attacks. It also provides some links to Identity Management. It mentions as the eighth recommendation the following: “Encourage Research into a standardization of Portable Reputation Systems” and emphasize the need for a standardized Transport Mechanisms for Reputation Data. However, none of these proposals tackle the issue of aggregated or federated reputation systems. The work presented in [23] deals with the problem of reputation systems for federations of online communities while taking into account privacy preserving issues.

There is no a uniform way to build reputation, however the project Venyo [32], released recently, tries to build a unified reputation value of a user who is a member of different systems. Also the OASIS Open Reputation Management Systems (ORMS) TC [19] is leading in this direction. The aim of this TC is to develop an ORMS that provides the ability to use common data formats for representing reputation data, and standard definitions of reputation scores. However, they do not intend to define algorithms for computing these scores, which is in our opinion an interesting open issue. This topic has also captured the attention of some identity federation solutions such as OpenID [21]. There is a proposal to extend OpenID in order to support exchange of reputation data [26].

3 Aims for Improving Reputation

Reputation helps to extrapolate the behaviour of a user in order to predict what these behaviours will be like in future actions carried out by such a user. Reputation is not a well defined concept as there is not a standard definition or way to measure it. In different scenarios the reputation of a user might have different meanings and can also be computed differently. Reputation is a rather global and subjective concept that depends on different factors such as the context where the user is performing the actions and the nature of these actions. Another important factor to take into account is the aim that leads users to improve their reputation, which might differ depending on their interests or the nature of the application and its context. It might be difficult to gather all the possible aims that lead a user to perform in order to improve his/her reputation. Below we provide a possible classification which we consider covers some of the most relevant aims for improving reputation. These classification has come out mainly as a result of matching the observation of the behaviour of the systems, more precisely, of the users of these systems.

Profit A higher reputation will directly provide more profit to the user. This is the model followed by eBay [7]. eBay is a popular online auction site where practically anyone can sell almost anything at any time. In eBay, the feedback represents a person's permanent reputation as a buyer or seller on eBay. It is built based on comments and ratings left by other eBay members who have sold or bought items to or from the member who has to be rated. There are three types of feedback ratings: positive, neutral and negative. The sum of these feedback ratings are shown as a number in parentheses next to the User ID. This feedback system has been updated recently with the intention of increasing buyer and seller accountability. eBay has eliminated the ability to produce negative ratings on buyers. Instead, sellers may contact the Seller Reporting Hub of eBay in order to solve disputes. Also neutral ratings will not be taken into account. Thus, suspended buyers can no longer negatively impact on a seller's record.

Reward A higher reputation will provide a reward to the user. This is the model followed by Epinions [10]. Epinions is a web site where members can write reviews, as well as other kinds of opinions. To post a review members must rate the product or service on a rating scale from 1 to 5 stars, one star being the worst rating, five stars being the best. For several years now, all opinions also come with a brief Pros and Cons section and a 'The Bottom Line'. In Social Science a rating scale is a set of categories designed to elicit information about a quantitative attribute. Epinions offers an 'Income Share' which ostensibly rewards reviewers for how much help they have given users on deciding to purchase products. All members can rate opinions by others as 'Off-Topic' (OT), 'Not Helpful' (NH), 'Somewhat Helpful' (SH), 'Helpful' (H), and 'Very Helpful' (VH). Opinions shorter than 200 words are called *Express Opinions* and rated 'Show' (S) or 'Don't Show' (NS). Members can also decide wether to 'trust' or to 'block' (formerly known as 'distrust') another member. All the trust and block relationships interact and form a hierarchy known as the Web of Trust. This Web of Trust (WOT) is combined with ratings in order to determine in what order opinions are shown. The order members see depends on their own ratings and their own trust and block choices. The order a visitor sees is determined by a default list of members a visitor supposedly trusts. The Web of Trust formula is secret.

Fear to retaliation This could be considered as a negative version of the previous bullet. In these cases if users act in such a way that cause negative effects on the site, and therefore, their reputation values decreased to certain threshold, they might be punished by the site administrators by reducing their privileges or access rights, or sometimes even by expelling them from the site.

This happens for instance, in forums. If the contents of the comments submitted by a certain user are not appropriate this user might be banned from the forum. This means this user will not be able to post any more comments for a certain amount of time. In case he repeats his behaviour the user can be expelled from the site.

World of WarCraft [20] is an online gaming community where fear of retaliation is an issue to users. Users with a low reputation in a given faction will be attacked on sight. Thus, keeping a high reputation will keep the user safe.

Ego A higher reputation does not give any profit to the user, but a higher status in the community and maybe some privileges not related to profit. This is the model followed by Advogato [1]. Advogato is an online community site dedicated to free software development, created by Ralph Levien. It describes itself as 'the free software developer's advocate.' Advogato was an early pioneer of 'online diaries', which later became known as blogs, and one of the earliest social networking web sites. Advogato combined the most recent entries from each user's diary together with a single continuous feed called the *recentlog*. Many high profile members of the free software and open source software movements are or have been users of this site.

The motivation behind Advogato was to try out in practice Levien's ideas about attack resistant trust metrics, having users to certify each other in a kind of peer review process and use this information to avoid the abuses that plague open community sites. Levien observed that his notion of attack resistant trust metric was fundamentally very similar to the PageRank [22] algorithm used by Google in order to rate articles interest. In the case of Advogato, the trust metric is designed to include all individuals who could reasonably be considered members of the Free Software and Open Source communities while excluding others.

It is worth to mention that we have identified these four factors as important factors that influence reputation, however, there could be others.

This distinction can help understanding the mechanisms to build trust upon reputation. The Reward model can be seen as an intermediate model between the Ego and the Profit models, and can be applied to any kind of community. One of the main difficulties when defining a reputation system is the definition of the mechanism for aggregating reputation values from different interactions. Some sites like Amazon [4] use the average. Other factors such as the value of the interaction and the reputation of the user providing the feedback could be also taken into account.

One way to classify reputation systems could be according to the aims that lead users to improve their reputation (as mentioned above). Another way could be according to the way reputation is computed, differentiating between centralized reputation systems where reputation is stored, updated and made available to other users in a central server; and distributed reputation systems where reputation is stored, distributed and usually computed on demand by collecting reputation values from the distributed system.

The importance of analyzing the aim for improving reputation resides in the relevance of the respective score. We are interested in aggregating reputation values from different sources and then investigating how to define the weights associated to them. A reputation value will be more valuable when the aim of the user for improving it becomes crucial for his interests.

We could represent these four factors in a two dimensional axis as depicted in Figure 1. The semi-axis correspond to the four factors we have proposed as an influence on reputation.

These are

$$(Ego, Reward, Fear, Profit)$$

Then, each system represented in the axis will have four vertices associated to it, which are $(e,0)$, $(-f,0)$, $(0,r)$ and $(0,-p)$, where e is the coordinate for Ego, f is the coordinate for Fear, r is the coordinate for Reward and p is the coordinate for Profit. Each of them represents the level of influence of the particular aim in the overall reputation of the system. If these vertices get connected we obtain a polygon that represents the reputation aims of the system. In order to make this representation homogeneous or normalized the addition of all the ”measurements” should be 1. This ”measurements” depend on the way reputation is computed in the system and they should be defined by the system itself. Note that the position of these factors in the axis does not mean they are conflicting concepts.

If we look at two different systems with clearly different aims such as Advogato and eBay we can provide an example of this graphical representation (see Figure 1). We can put in relevance that for the Advogato site the Ego factor is of a high influence whereas it is of a very little influence for the case of eBay (as we mentioned above). Thus, as eBay is a mainly Profit oriented site, this is reflected in the corresponding axis of the Figure.

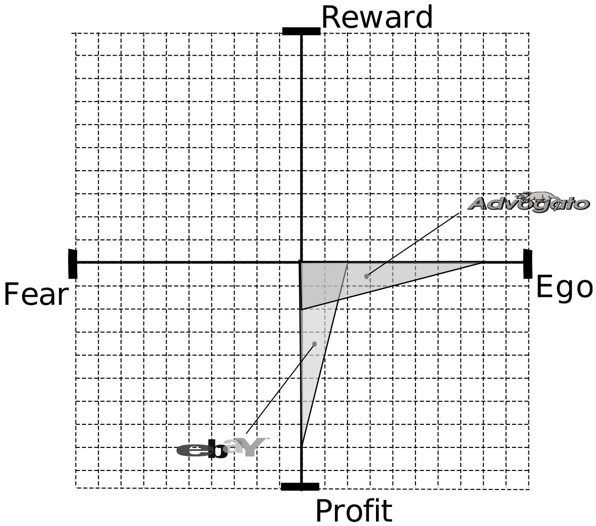

Figure 1: Dimensions of Reputation

Each reputation value is associated to the above defined dimensions by means of the *Reputation Definition Vector*. Note that we used for our example as a base for the reputation definition vector $(Ego, Reward, Fear, Profit)$ but there might be others that can be used for this purpose.

Definition 1 (Reputation Definition Vector - RDV)**.** *The vector that has as coordinates each of the relative weights for the given reputation base is called a Reputation Definition Vector. A reputation definition vector is a vector* $\overline{v} = (v_1, \ldots, v_n) \in [0,1]^n$ *such as*

$$\sum_{i=1}^{n} v_i = 1$$

4 Federated Reputation System

The reputation engines maintained by some networks depend very much on the context of the network such as social communities, eBay or some engine proper of a specific company that carried out a specific task (see [16] for a survey on reputation engines). Assuming there are different reputation evidences for a user but in different contexts we might be interested in obtaining a unique value as an overall of the different reputation values. This can not be as simple as adding these evidences as they were obtained in different contexts. We should find a 'similarity' among these evidences in order to be able to compute a reputation value for a different context.

Federated reputation systems are raising some interest in the area of online communities and services, however, the development of federated reputation systems is still in its inphancy. There are already existing approaches that aim to build a unique reputation from different reputation sources. In [23] the authors set the preconditions for designing an interoperable reputation system for online communities. A similar approach is followed in [6] where the author tries to solve the problem of free-riding in BitTorrent by using reputation. He considers that any BitTorrent network behaves as a federation and calculates the reputation within the federation. Venyo is another attempt to create a kind of a federated reputation system. Venyo [32] is an organization that offers a universal online reputation service. The reputation is expressed in the form of a personal reliability index - the Vindex$^{\mathrm{TM}}$- which is based on the evaluation by the community of the user's web contributions such as blog posts, pictures or videos, etc. Users registered at Venyo link their Venyo profile to the identities they use in the sites used as a source of reputation.

Our approach is slightly different. We propose an Identity Federation model where there exists an Identity Provider (IDP). Thus, a user is identified by his/her IDP in any context with a unique identity within the federation. This IDP will keep reputation of a user by maintaining a Reputation Manager engine. We call this model *Federated Reputation Model*.

Figure 2 shows the architecture of the proposed model. In this model a user will request a service from a Service Provider (SP), either *Federated Service* 1 or 2 in the Figure (step 1). After that, the user will be redirected to its IDP for authentication (step 2). Then, once the IDP has successfully authenticated the user, this will be again redirected to the SP, but with the proper credentials (step 3). This is the usual way Identity Federation systems work, which is represented as a continuous line. However, we propose an extra step, step 4, for our model where the IDP includes a *Reputation Engine* that stores and updates reputation values coming from different service providers. This reputation values can be provided back to the SP as user attributes when requested.

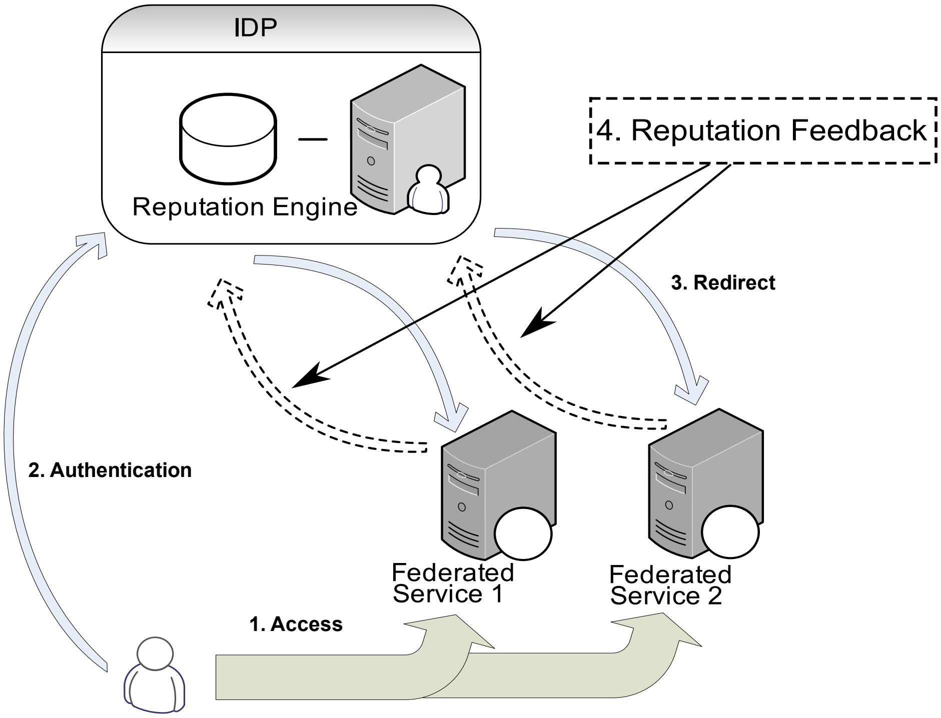

Figure 2: Federated Reputation Model

This extra step is represented by dashed arrows.

Prior to be able to participate in the feedback system, the SP has to define a proper reputation definition vector that classifies somehow the expected behaviour of the user with respect to reputation within its services. This information is added to the actual metadata needed for setting the identity federation.

Apart from that, the IDP has to maintain a database of reputation values. This database stores, for each user, the reputation that such a user holds in each of the SPs that have provided reputation feedback about such a user.

4.1 Computation of the Federated Reputation

Let us assume a scenario where different service providers might hold some information about reputation of a user, u, in the identity federation that is managed by the IDP. In our approach the reputation engine is managed within the IDP. The purpose of this engine is to calculate a federated reputation value for users managed by this IDP. This federated reputation value takes into account the reputation history of the users.

Definition 2 (Federated Reputation Value)**.** *The Federated Reputation Value is calculated as*

$$fr_B(u) = \sum_{i=1}^{n} \frac{r_{A_i}(u)w(A_i,B)}{\sum_{i=1}^{n} w(A_i,B)}$$

where

- *n represents the number of service providers that feed the IDP with reputation information about user u,*
- *$r_{A_i}(u)$ is the reputation value stored for user u regarding service provider A_i and*
- *$w(A_i,B)$ is the weight assigned to how 'similar' or 'close' the different service providers, A_i, are to B .*

The most important parameter of the previous formula is the weight that measures the similarity of two SP with regard to the aim of their users to improve reputation. This weight ranges from 0 to 1 where 0 is assigned when two service providers are not related at all and 1 when they share the same aim. Then, when computing the federated reputation, all the reputation values coming from irrelevant SPs (i.e. those which are not similar at all to the targer service provider) will not be taken into account as their weight will be 0.

In Figure 1 we showed a two dimensional representation of the reputation definition vector (RDP), which is indeed a four dimensional vector. This representation helps us decide whether two services have a common aim for reputation by looking at the quadrilaterals that represent both services, but does not help us giving a precise measure for this similarity. For this purpose we can use the norm in $\mathbb{R}^4$. Let us assume that the reputation definition vector of the target SP, B, is represented by v_0 and that v_i represents the reputation definition vector of the SP A_i. Then, the similarity weight is calculated as follows:

$$w(A_i,B) = 1 - \|\overline{v}_i - \overline{v}_0\| \tag{1}$$

Thus, as expected, if a RDV of a service provider is close to the one of the target service then $\|v_i - v_0\|$ is close to 0 and, therefore the similarity weight i.e., $w(A_i,B)$ will be close to 1.

It is difficult to show how distances work in a four dimensional space, but if we focus on two of the coordinates of the reputation definition vector, the situation is depicted in Figure 3.

In Figure 3 we have represented three reputation definition vectors for three services: Advogato $(0.2,0.8)$, eBay $(0.8,0.2)$ and Epinions $(0.5,0.5)$. We have subjectively considered Advogato to be more Ego oriented, whereas eBay can be considered more profit oriented. Regarding Epinions we could say that it is neutral with regards to those two factors. The actual reputation definition vectors have to be provided by the service provider. Here we only provide an example. There is also a fourth service provider that is our target service provider with a reputation definition vector $(0.3,0.7)$.

In order to compute the federated reputation value for the target service provider we need to compute first the similarity weights:

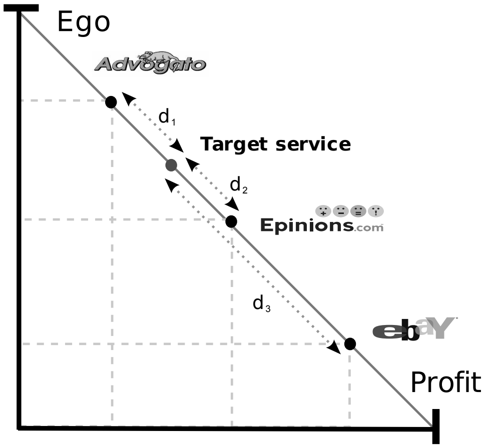

Figure 3: Distances between Reputation Definition Vectors

- $w_1 := w(Advogato, Target) = 1 - d_1 = 1 - \|(0.2, 0.8) - (0.3, 0.7)\| = 0.86$
- $w_2 := w(Epinions, Target) = 1 - d_2 = 1 - \|(0.5, 0.5) - (0.3, 0.7)\| = 0.72$
- $w_3 := w(eBay, Target) = 1 - d_3 = 1 - \|(0.8, 0.2) - (0.3, 0.7)\| = 0.30$

Let us assume that two users, u_0 and u_1, have the following reputation values 0.8 , 0.5 and 0.3 for u_0 and 0.3 , 0.5 and 0.8 for u_1 in Avogato, Epinions and eBay respectively.

Then, the federated reputation values of these two users in the target service provider are,

$$f_B(u_0) = \frac{0.8 \cdot 0.86 + 0.5 \cdot 0.72 + 0.3 \cdot 0.3}{1.88} = 0.6$$

and

$$f_B(u_1) = \frac{0.3 \cdot 0.86 + 0.5 \cdot 0.72 + 0.8 \cdot 0.3}{1.88} = 0.45$$

As expected, user u_0 whose reputation in the closer providers, i.e. Advogato and Epinions was better than the reputation of u_1, obtains a better federated reputation value for the target service B.

The reputation value computed in Definition 2 can be used as an initial reputation value when the user first accesses a new service or as a reputation value for services without a reputation engine. In any case, the federated reputation value is an estimation of the expected behaviour of the user. This estimation will be more accurate when all the available information for the computation corresponds to very close service providers. The accuracy of this estimation can be measured by the mean of the distances of all the observations. In the example above the accuracy of the estimation is as follows,

$$\frac{w_1 + w_2 + w_3}{3} = \frac{1.88}{3} = 0.62$$

There might be other alternatives in order to obtain the federated reputation value, however we believe the approach we follow has a good balance between expressiveness and complexity.

The reputation engine might incorporate mechanisms to filter out reputation values that come from service providers that are only marginally related. This will make the federated reputation function more robust. Thus, in the example above we could apply a filter that only considers as useful those values of w_i such as $w_i > 0.5$. Then, only w_1 and w_2 are the considered values and the value assigned to eBay is not considered as a relevant service provider.

Then the new federated reputation values of these two users in the target service provider are,

$$f_B(u_0) = \frac{0.8 \cdot 0.86 + 0.5 \cdot 0.72}{1.58} = 0.66$$

and

$$f_B(u_1) = \frac{0.3 \cdot 0.86 + 0.5 \cdot 0.72}{1.58} = 0.39$$

The value for user u_0 has been increased as the filter ruled out a low reputation value whereas the value for u_1 has been decreased as the one removed after applying the filter was a high reputation value.

The accuracy of the estimation is in this case

$$\frac{w_1 + w_2}{2} = \frac{1.58}{2} = 0.79$$

which has been increased.

Another parameter useful for estimating the robustness of the federated reputation value is the number of evidences taken into consideration. We have to find a balance between accuracy, defined as a mean of the weights, and the number of evidences used for the computation of the federated reputation value.

5 Building Trust from Federated Reputation Systems

The ultimate purpose of the introduction of the Federated Reputation system presented in Section 4 is to build trust of the members of the federations. We believe this way of building trust can be useful when users can interact among them.

5.1 Site to User Trust

Federation of identities has been an issue in the past few years. Some of the proposals that aim at achieving Identity Federations are Higgins project [13], Windows

CardSpace [5], Shibboleth [28] or OpenID [21]. This way, a user does not necessarily need to perform a registration process in each site but the identity of the user can be transferred somehow from one member to the federation to another. This concept is also related to the single sing-on feature.

Unfortunately, none of the proposals mentioned above provide a link to the reputation systems that may be running on the user central registration site or even on the federated sites. It is true that the reputation on the central registration site might be transferred as a user attribute but the reputation obtained on the federated sites is not considered in any way.

5.2 User to User Trust

Sometimes it is difficult to decide who to trust. It is even more difficult when we use second hand information for the entity to be trusted. In those cases we can use information regarding to the reputation of users in order to decide whether to trust them or not. Moreover, we could, after that, trust their trustees (or users they trust) following recommendations. This procedure will help expanding our trust circle. This is specially useful when the SPs are social communities. In these cases users can interact among them and therefore the exchange of reputation values can take place without having to necessarily do it through the SP.

It is difficult to derive a trust value only based on reputation. Normally, reputation is linked to some kind of activity and we may wonder whether to trust a user regarding to a different and independent context. In case there is not a reputation value related to the context we are dealing with, we have to first consider the reputation of the user out of the context by combining values from different and heterogeneous contexts (see Section 4.1). This way we detach the context from the reputation value. Moreover, if we apply the method introduced in the aforementioned section we can assign an appropriate weight to all the reputation values accordingly and therefore, we can derive a better trust value for this user.

6 Conclusions and Future Work

In this paper we have introduced a federated reputation model that can be used in order to derive trust. Besides the usual way Identity Federations work, we propose to add an additional step to them in such a way that once the identity of the users have been provided by the IDP to the SP, the latest could also provide the IDP with additional information about the reputation of a given user that will be maintained by the IDP. The reputation values are stored and managed by the IDP by using a reputation manager located in it.

In this scenario users registered with the federation can benefit from the already existing reputation values on their IDP in order to gain access to a given service offered by a SP member of the federation. We have based our approach on the way the factors that influence reputation can be represented. Thus, we allocate these factors into an n- dimensional axis representation, which also allows us to calculate the relationship between the different service providers by calculating the distances between them with respect to these axis.

Using these reputation values trust can be built from user to user and from a site to the user. This latter case might be easier to handle as the scope of reputation is wider. On the user to user interactions scenario we have to solve several issues regarding to the subjectivity of the computed reputation value.

Our model considers that the IDP is a trusted entity and thus, privacy is not a a problem for it. However, we are aware that in an ideal solution the reputation manager might not be hosted in the IDP and therefore, some privacy issues may arise. Investigating this other approach could be a very interesting challenge worth to be investigated in the future.

There are several research initiatives in the field of social and online communities that focuses on trust establishment issues where we are interested in applying our model. One of such approaches is the PICOS project[24]. The ideas presented in this work may also help research on the topic of networked enterprisers or alliances, where reputation might help building those alliances in an optimal way, selecting the 'best' reputed companies for each task. One of such approaches is the SPIKE project[25].

References

[1] Advogato. http://advogato.org/.

[2] I. Agudo, C. Fernandez-Gago, and J. Lopez. An Evolutionary Trust and Distrust Model. In *4th Workshop on Security and Trust Management*, Electronic Notes in Theoretical Computer Science, Trondheim, Norway, 2008.

[3] Florina Almenarez, Andres Marin, Daniel Dyaz, and Juan Sanchez. Developing a Model for Trust Management in Pervasive Devices. In *PERCOMW '06: Proceedings of the 4th annual IEEE international conference on Pervasive Computing and Communications Workshops*, page 267, Washington, DC, USA, 2006. IEEE Computer Society.

[4] Amazon. http://www.amazon.com/.

[5] Microsoft CardSpace. http://msdn.microsoft.com/en-us/library/aa480189.aspx.

[6] Jaime Perez Crespo. Aretusa: Sistema de reputacion para bittorrent. Master's thesis, Universidad Rey Juan Carlos, 2008.

[7] eBay. http://www.ebay.com.

[8] ENISA. Position paper no.1 Security Issues and Recommendations for Online Social Networks.

[9] ENISA. Position paper no.2 Reputation-based Systems: a Security Aanalysis.

[10] Epinions. http://www.epinions.com.

[11] Facebook. http://www.facebook.com.

[12] R. Falcone and C. Castelfranchi. The Socio-Cognitive Dynamics of Trust. In *4th Workshop on Agents- Trust in Cyber-Societies*, volume 2246 of *Lectures Notes in Computer Science*, pages 55–72, Barcelona, 2001. Springer-Verlag.

[13] Freehaven. Freehaven. http://www.eclipse.org/higgins/.

[14] P. Herrmann and H. Krumm. A Framework for Modeling Transfer Protocols. *Computer Networks*, 34(2):317–337, 2000.

[15] Peter Herrmann. Temporal Logic-Based Specification and Verification of Trust Models. In Ketil Stølen, William H. Winsborough, Fabio Martinelli, and Fabio Massacci, editors, *Trust Management, 4th International Conference, iTrust 2006*, volume 3986 of *Lecture Notes in Computer Science*, pages 105–119, Pisa, Italy, 2006.

[16] A. Jøsang, R. Ismail, and C. Boyd. A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, 43(2):618–644, 2007.

[17] Zhaoyu Liu, Anthony W. Joy, and Robert A. Thompson. A Dynamic Trust Model for Mobile Ad-Hoc Networks. In *FTDCS '04: Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems*, pages 80–85, Washington, DC, USA, 2004. IEEE Computer Society.

[18] L. Mui. *Computational Models for Trust and Reputation:Agents, Evolutionary Games, and Social Networks*. PhD thesis, Massachusetts Institute of Technology, 2003.

[19] OASIS. http://www.oasis-open.org/committees/orms.

[20] World of Warcraft. WOW. http://www.worldofwarcraft.com/info/basics/reputation.html.

[21] OpenID. http://openid.net/.

[22] Google PageRank. http://www.mipagerank.com/.

[23] Franziska Pingel and Sandra Steinbrecher. Multilateral Secure Cross-Community Reputation Systems for Internet Communities. In S. K. Katsikas S. M. Furnell and A. Lioy, editors, *Trust, Privacy and Security in Digital Business, TrustBus08*, volume 5185 of *LNCS*, pages 69–78, Turin, Italy, September 2008.

[24] PICOS Project. http://www.picos-project.eu/.

[25] SPIKE Project. http://www.spike-project.eu/.

[26] OpenID Reputation Service. http://myidproject.net/?openidreputationservice.

[27] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara. Reputation Systems. *Communications of ACM*, 43(12):45–48, 2000.

[28] Shibboleth. http://shibboleth.internet2.edu/, Visited on 11/6/2009.

[29] TERENA. http://www.terena.org/activities/tf-emc2/docs/tf-emc2-tor08-10.pdf.

[30] Tuenti. http://www.tuenti.com/.

[31] J. Ubois. Online Reputation Systems. In *in Release 1.0*, volume 21. www.edventure.com, 2003.

[32] Venyo. http://www.venyo.org/.

[33] Stanley Wasserman, Katherine Faust, and Dawn Iacobucci. *Social Network Analysis : Methods and Applications (Structural Analysis in the Social Sciences)*. Cambridge University Press, November 1994.