Portable reputation: Proving ownership of reputations across portals

Sandeep S. Kumar and Paul Koster

Information and System Security Group
Philips Research Laboratories, Eindhoven, The Netherlands
{Sandeep.Kumar,R.P.Koster}@philips.com

Abstract. User reputation has become a valuable commodity for enabling trusted transactions on the Internet especially with strangers in virtual communities. However, the reputation information about the various users are normally locked-up in the silos of different web-portals where the members interact. This effectively creates multiple reputation ratings for the same user, each one painstakingly built over a long time at each web-portal. Though this status quo is favorable for established web-portals as it enables them to lock-in their customers, consumers have a strong interest in a portable reputation system that allows them to cross the boundaries of the competing portals. In this paper, we present a portable reputation mechanism which is managed by the users on their own with minimal co-operation from the web-portals. This method enables a user to combine from various portals the reputation information of others, which are proven to belong to them in a reliable and cryptographically secure way. Users can appropriately weigh the reputation from different web-portals according to their individual choice and trust in the different web-portals. The solution has the advantage that it does not require any unified reputation rating framework implemented by all web-portals. Additionally the cryptographic binding is constructed such that it prevents users to form a coalition and share their good reputation ratings among them.

1 Introduction

In today's Internet connected society, it has become more common to have new forms of interactions with complete strangers. These virtual interactions can be for various purposes like getting the right information (like Yahoo answers), for real value transactions (like Ebay), and many more. All such interactions with strangers require some amount of trust in the other party which goes beyond the knowledge of their virtual pseudonymous identity. In fact, to encourage these forms of stranger-stranger interactions, web-portals use reputation based systems which are normally some form of numerical ratings of the past behavior. The reputation system functions by collecting, aggregating and distributing the historic behavior of the participating entities of the web-portal. Resnick et. al. [6] mention three properties that a reputation system requires at a minimum:

1. Participating entities are long-lived, so that there is an expectation of future interaction.
2. Feedback about current interactions between entities are captured and distributed. Such information must be visible in the future.
3. Past feedback should guide new interaction decisions. Therefore entities must pay attention to the reputation while making their decisions.

Ebay is an example where the reputation system is attributed to its phenomenal success in enabling real valued auctions between complete strangers [2]. The reputation information in such systems gives the parties involved in the interaction the much needed help in deciding whom to trust, encouraging trustworthy behavior to maintain high reputation, and deter participation of cheater and unskilled parties. Reputation therefore has become an extremely valuable commodity which enables higher price premiums in identical transactions [7] and people work hard to earn reputation on these portals. Consequently for web-portals, reputation not only enables new transaction models and possibilities but also provides the ability to lock-in customers. Customers who have worked hard on creating a good reputation on a portal are less likely to switch to another portal unless the benefit is substantially more than the effort required to recreate a similar good reputation. However, a user switching to a new portal not only needs to painstakingly rebuild his reputation but also has to lose out on his higher price premium which he would have been entitled based on his higher perceived trustworthiness. These silos of reputation can follow from a combination the reasons listed below.

1. Different portals cannot securely verify if the pseudonyms used on both portals actually belong to the same user. This can be partially solved if a federated identity management system is in place. However, this does not scale well with the large number of portals which need to be within the *circle of trust* of the federated identity provider.
2. Portal owners realize that the painstakingly generated reputation ratings enable them to lock-in users to their portal and hence would not easily participate in a federated system in which they need to share detailed information about their users with possible competitors.
3. Different portals use completely different reputation rating frameworks which do not directly map to each other. The different frameworks are used because each web-portal considers different aspects as important to rate trustworthy behavior. Other reason can also be due to the wide variety of ways that the reputation systems can be attacked [4] and by making a system closed and controllable, some of the attacks can be thwarted.

However, portability of reputation data can be of utmost importance to consumers. Due to the reputation lockup, consumers are implicity forced to use their current portals for their interactions even if they find other new portals more attractive. An alternative for this is to have a centralized server which handles all the reputation data of users across portals (a similar idea is mentioned in [6], tried by virtualfeedback.com and now defunct). The problem with a centralized approach is that different systems require different reputation frameworks as mentioned before. The OASIS Open Reputation Management Systems (ORMS) Technical Committee [1] is trying to address standardization and interoperability of information used to derive reputation ratings for individuals and institutions participating in Internet communities. However there are other reasons too which favor a controlled closed system, for example, it is hard to make sure that the reputation ratings are being provided by actual transaction partners, which can be reliably verified only by the web-portal where the transaction had occurred.

1.1 Our Contribution

In this paper, we map the problem of portability of reputation information to users wanting to show other entities their reputation ratings on different web-portals and prove that those belong to him/her. It is normal for the reputation information of an user of a web-portal to be publicly visible to everyone. It associates the reputation information to the user's pseudonym on the portal. Therefore proving possession of reputation can be addressed by proving possession of the pseudonym at the portal. The entity to whom the reputation ratings are shown can decide how to weigh those ratings based on their trust in the originating portal or their trust metric (based on context of the present interaction).

The method described in the paper enables users to easily claim their local reputation at various web-portals by provably presenting the possession of pseudonyms to a requesting entity to increase the level of trust in an interaction. The requesting entity could be a new transaction partner or a web-portal allowing users to initially use the reputation data from other web-portals to reduce the burden of starting off as an unknown entity.

The paper is organized as follows: in Section 2 we specify the problem and assumptions of the system. We outline the solution in Section 3 and in Section 4 we present some cryptographic preliminaries and the protocol details. Some applications are presented in Section 5 and conclusions are presented in Section 6.

2 Problem definition

Users normally have different pseudonyms at different web-portals where they engage in transactions and earn reputation. For example, an user *Alice* can have pseudonyms $P1$, $P2$ and $P3$ on three different portals $S1$, $S2$ and $S3$ respectively as shown in Fig. 1. These pseudonyms can be directly linked to a real user if personally identifiable information is revealed (like Alice's name or email-address) along with the pseudonyms. However, it is also very easy for an impersonator to claim to be Alice on a different portal by mentioning the corresponding personally identifiable information. Hence the link-ability is not strong unless such information is cryptographically signed. Furthermore, making such personal information public leads to the problem of privacy. Most users tend to have non-identifiable pseudonyms on different portals for privacy reasons to avoid linking

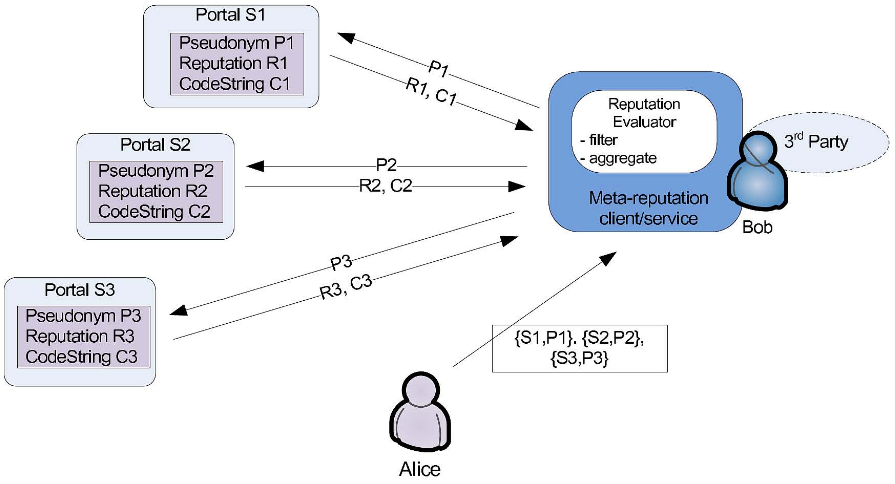


Fig. 1. Architecture for portable reputation

of profiles and their actions on these portals. Cryptographic signatures can only further help in this linking process and consequently reduce privacy. Anonymous linking of pseudonyms is possible if a trusted identity provider is acting as the pseudonym provider (or identity provider) for all the portals as is the case in federated identity management. However, most of the time services are competitors who value their customer base and do not trust each other. This leads to the need for a solution where the user Alice would like to reveal possession of the pseudonyms $P1$, $P2$ and $P3$ to a 3rd party like *Bob* without the active involvement of the web-portals $S1$, $S2$ and $S3$. This enables Alice to claim her reputation $R1$, $R2$ and $R3$ at the various portals and reliably prove to Bob as belonging to her. Bob can then decide how to combine these reputation ratings from different portals based on his trust in how reputation is evaluated at these portals or based on the nature of the current interaction with Alice.

3 Solution Outline

The main goal of the solution is to allow users to make their reputation portable on their own with minimal interaction between portals. The first step in the process is for the user (here Alice) to create some form of a coded string and attach it to her pseudonym in a publicly accessible way (e.g. the user profile page of Alice as shown in Fig. 1 as $C1$, $C2$ and $C3$). The purpose of this coded string is to enable Alice to prove that she possesses the corresponding pseudonyms and therefore the associated reputation. This coded string needs to satisfy the following requirements:

1. The coded string contains a secret that only the user (Alice) is aware of and can prove knowledge of it (preferably without revealing the secret)
2. The coded string should be bound to the user (Alice) in such a way that she cannot transfer her reputation to other users without revealing a secret that compromises all of her other pseudonyms
3. The coded string should not be a source of information to enable linking of pseudonyms by third parties not involved in the transaction with the user (Alice).

To help Bob verify the coded string, we define a meta-reputation (meta-RS) client to which Alice can provably claim all the pseudonyms as belonging to her. The meta-RS also enables the aggregation of the reputation ratings based on Bob's preferences. An alternative is to consider the meta-RS to be a trusted third party which both parties trust to perform truthfully all the various verification operations. The meta-RS as an intermediate trusted party is suitable in environments where Alice does not want to reveal her pseudonyms to Bob but only wants to give Bob the possibility to get an aggregate reputation value based on his preferences. The other advantage of a trusted intermediary is that no client is required at the transacting party Bob and instead could be a third party web-site which performs all the operations of the meta-RS client.

4 Detailed Protocol Description

Before we describe the solution, we first present the relevant cryptographic concepts that constitute the solution.

4.1 Cryptographic preliminaries

The main underlying concept is the computational hardness of the discrete logarithm (DL) problem which is defined as follows

Definition 1 *Given a finite group* $\mathbf{G}$*, g the generator element, and* $e \in \mathbf{G}^*$*, find m such that* $g^m = e$*.*

The DL problem exists in any group, however when used for cryptographic purposes the group is usually chosen as the multiplicative group of integers modulo N, $\mathbb{Z}_N^*$, where N is chosen to be a relatively large prime. Various well established public-key cryptosystems are based on the DL problem like the ElGamal [3] system and the Digital Signature Standard (DSS) [5].

Based on the DL problem is the equally hard Diffie-Hellman (DH) problem which is defined as

Definition 2 *Given a finite group* $\mathbf{G}$*, g the generator element, and randomly chosen* $x, y \in \mathbb{Z}$*. Given* g^x *and* g^y*, find* g^{xy} *.*

4.2 Pseudonym ownership protocol

We present here one method to generate the coded string that can fulfil the requirements mentioned before. For the representation of the coded string and the protocol, we use the following notation

1. N is a prime and all arithmetic is performed in the multiplicative group of integers modulo N. N is chosen relatively large to be secure based on the hardness of the discrete logarithm problem. N is publicly known.
2. g is a generator of the multiplicative group modulo N. g is publicly known.
3. $H[\,]$ is a hash function, e.g. SHA-256
4. I is the user and U_I is the unique secret known only to him.
5. P_i are the pseudonyms associated with user I at web-portals S_i
6. K_i are the unique secrets associated with each pseudonym P_i
7. a and b are random numbers

The coded string used by user I (say Alice) for the pseudonym P_i is the pair constructed as follows $\mathbb{C}_i = (\bar{c}, \hat{c}) = (g^{K_i}, g^{U_I K_i})$.

Alice wants to prove to a third party (say Bob, who could also be a web-portal) that a set of pseudonyms at web-portals $\mathbb{P} = \{\{P_1, S_1\}, \ldots, \{P_n, S_n\}\}$ belongs to her and therefore the corresponding reputation which is publicly visible at these portals. The protocol is shown in detail in Fig. 4.2 and each of the steps is described further.

Bob chooses a random number a which he keeps secret to himself and sends the value $\alpha = g^a$ to Alice. Alice cannot determine a from α based on the discrete log problem. However Alice can use her secret K_i to derive $\alpha^{K_i} = g^{a*K_i}$. Bob similarly has the value $\bar{c} = g^{K_i}$ but not the value K_i. Bob performs a similar step $\bar{c}_i^a = g^{K_i*a}$. Hence now Alice and Bob have the same value. An additional hashing is done by Alice to derive $\nu_i = H[\alpha^{K_i}]$ and sends it to Bob. If Bob can verify that ν_i is same as the hash value he generates $\tau_i = H[\bar{c}_i^a]$, then it is clear to Bob that Alice knows the secret and has access to the pseudonym. This step is performed for each of the pseudonyms that Alice shows to Bob.

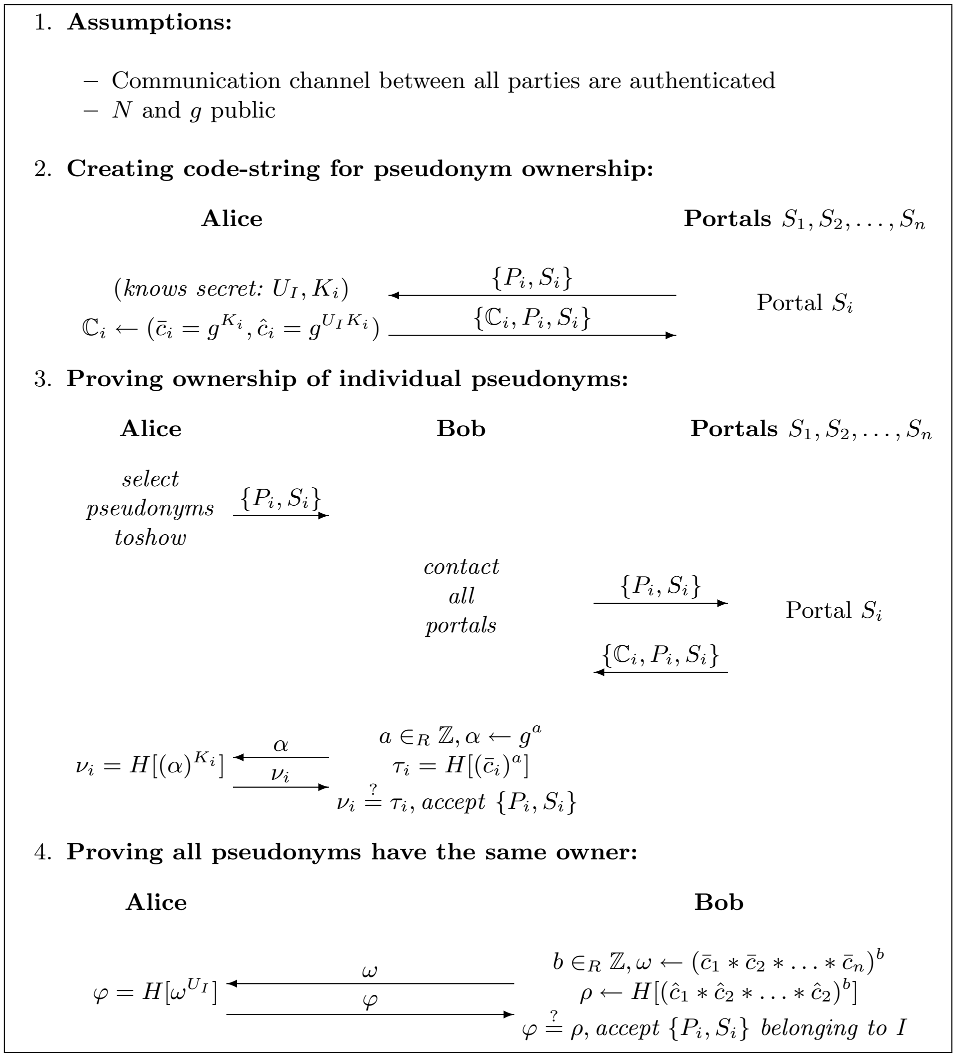
However, the fact that Alice knows the secret for each individual pseudonym does not prohibit Alice to form a coalition with multiple people and use a secret of an account belonging to a member of the coalition for this particular interaction. Therefore Bob needs to be convinced that all accounts have something in common (here the secret U_I) that is known only to Alice.

Now Bob chooses a random number b which he keeps as secret to himself and computes

$$\begin{aligned}\omega &= (\bar{c}_1 * \bar{c}_2 * \ldots * \bar{c}_n)^b \\ &= (g^{K_1} * g^{K_2} * \ldots * g^{K_n})^b \\ &= g^{(K_1 * K_2 * \ldots * K_n) * b}\end{aligned}$$

and sends ω to Alice. Alice now computes

$$\begin{aligned}\varphi &= H[\omega^{U_I}] \\ &= H[(g^{(K_1 * K_2 * \ldots * K_n) * b})^{U_I}] \\ &= H[(g^{(K_1 * K_2 * \ldots * K_n) * b * U_I}]\end{aligned}$$



1. **Assumptions:**
   - Communication channel between all parties are authenticated
   - N and g public
2. **Creating code-string for pseudonym ownership:**

Alice
Portals $S_1, S_2, \ldots, S_n$
(*knows secret:* U_I, K_i)
$\{P_i, S_i\}$
Portal S_i
$\mathbb{C}_i \leftarrow (\bar{c}_i = g^{K_i}, \hat{c}_i = g^{U_I K_i})$
$\{\mathbb{C}_i, P_i, S_i\}$

3. **Proving ownership of individual pseudonyms:**

Alice
Bob
Portals $S_1, S_2, \ldots, S_n$
select pseudonyms toshow
$\{P_i, S_i\}$
contact all portals
$\{P_i, S_i\}$
Portal S_i
$\{\mathbb{C}_i, P_i, S_i\}$
$a \in_R \mathbb{Z}, \alpha \leftarrow g^a$
$\tau_i = H[(\bar{c}_i)^a]$
$\nu_i = H[(\alpha)^{K_i}]$
α
ν_i
$\nu_i \overset{?}{=} \tau_i$, *accept* $\{P_i, S_i\}$

4. **Proving all pseudonyms have the same owner:**

Alice
Bob
$b \in_R \mathbb{Z}, \omega \leftarrow (\bar{c}_1 * \bar{c}_2 * \ldots * \bar{c}_n)^b$
$\rho \leftarrow H[(\hat{c}_1 * \hat{c}_2 * \ldots * \hat{c}_2)^b]$
$\varphi = H[\omega^{U_I}]$
ω
φ
$\varphi \overset{?}{=} \rho$, *accept* $\{P_i, S_i\}$ *belonging to* I

Fig. 2. Pseudonym ownership protocol

and sends φ to Bob.

Bob can check if all pseudonyms belong to Alice by first computing

$$\begin{aligned}\rho &= H[(\hat{c}_1 * \hat{c}_2 * \ldots * \hat{c}_2)^b] \\ &= H[(g^{U_I K_1} * g^{U_I K_2} * \ldots * g^{U_I K_n})^b] \\ &= H[(g^{(K_1 * K_2 * \ldots * K_n) * U_I * b}]\end{aligned}$$

If $\varphi = \rho$, it proves that Alice possesses the secret U_I and hence proves that all the pseudonyms belong to her. The main reason that prevents sharing of pseudonyms across users is that once a pseudonym is shared that Alice also has to reveal her unique secret U_I, which compromises the security of all her other pseudonyms.

Once Bob is convinced about the ownership of the pseudonyms by Alice, he can contact the portals to retrieve the publicly visible reputation ratings of each of the pseudonyms. Bob's meta-RS can combine these ratings based on the context in which he is interacting with Alice and on his other personal preferences like weights for different portals.

However, it is important to realize certain limitations in the methodology, like users not revealing their pseudonyms with bad reputation. Our intention is not to capture all possible reputation of the user but to give users the ability to prove possession of any reputation they claim to be theirs and leave the the final decision to the users who will need to weigh it for their transactions.

5 Applications

Possible applications of the presented portable reputation mechanism include online services and emerging pervasive applications. Today, rating and reputation-based online services include online auctions, discussion forums, questions-and-answers boards, and review services. These services have in common that users build up a reputation by participating in transactions. Using the portable reputation mechanism enables users to leverage reputation for a broader range of online services, illustrating a typical case of user-centric identity. For example, it would enable somebody to incidentally buy or sell something on a niche site while also presenting his reputation from e.g. E-bay. For this purpose the user subscribes to an independent reputation aggregation service (meta-RS) trusted by both parties. This ensures that he can use his standard browser and avoids the need for a client-side extension. The user establishes an account at this meta-RS service and indicates at which services he holds a reputation. The meta-RS calculates the coded string and instructs the user to include them in his profile at the individual services. Subsequently, a transacting entity and the meta-RS can perform the ownership protocol, enabling the user to bootstrap his reputation in a trustworthy way. The meta-RS service can also present an aggregated reputation omitting the details of the full protocol and hence preserving privacy. It then presents the transacting party with the most relevant and useful information, which may involve selection, annotation and post-processing of reputation according to certain rules to form an aggregate value.

Pervasive applications like monitoring and coaching or independent living are a second class of applications that benefit from a portable reputation mechanism. The combination of sensor-based monitoring and interactions in the physical environment as well as a rich set of third party services makes trust very important. However, these applications tend to build up reputation less quickly since the transaction frequency is lower and distributed over different contexts. Portable reputation would enable a user to leverage his longstanding reputation at a variety of review services and discussion forums for e.g. a peer-coaching service using reputation-based trust between community members. In this class of applications reputation portability may be facilitated by the user's personal device having a meta-RS client in addition to its functions to aggregate sensor information and interact with services and devices in the physical environment. The personal device and the services can execute the portable reputation protocol. The protocol may also be executed in a peer-to-peer model between users' devices.

6 Conclusions

We presented a method through which users can prove ownership of their reputation across web-portals. We assumed a model of minimal co-operation of web-portals and created a user-centric protocol. The portable reputation mechanism is managed by the users on their own with minimal co-operation from the web-portals. Users can prove to each other (or other parties) in a reliable and cryptographically secure way the possession of the various individual reputation ratings without requiring any unified reputation rating framework implemented by all web-portals. Additionally the cryptographic binding is constructed such that it prevents users from sharing their reputation ratings with others. We also present some application scenarios where it could be used.

References

1. *OASIS Open Reputation Management Systems (ORMS) Technical Committee.*
2. Jennifer Brown and John Morgan. Reputation in online markets: The market for trust. *California Management Review*, 49(1):61–81, 2006.
3. Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 10–18, New York, NY, USA, 1985. Springer-Verlag New York, Inc.
4. ENISA. Reputation-based systems: a security analysis. Technical Report 2, ENISA Position Paper, 2007.
5. CORPORATE NIST. The digital signature standard. *Commun. ACM*, 35(7):36–40, 1992.
6. Paul Resnick, Ko Kuwabara, Richard Zeckhauser, and Eric Friedman. Reputation systems. *Commun. ACM*, 43(12):45–48, 2000.
7. Paul Resnick, Richard Zeckhauser, John Swanson, and Kate Lockwood. The value of reputation on ebay: A controlled experiment. *Experimental Economics*, 9(2):79–101, June 2006.