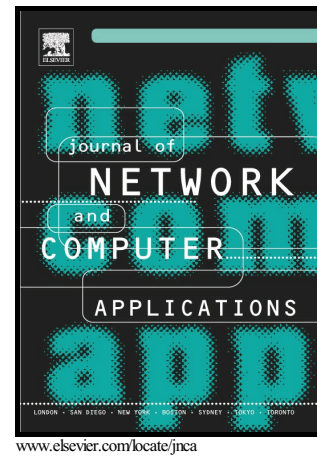


A privacy-preserving reputation system with user rewards

N. Busom, R. Petrlc, F. Sebé, C. Sorge, M. Valls



PII: S1084-8045(16)30332-0
DOI: <http://dx.doi.org/10.1016/j.jnca.2016.12.023>
Reference: YJNCA1806

To appear in: *Journal of Network and Computer Applications*

Received date: 27 November 2015
Revised date: 13 September 2016
Accepted date: 12 December 2016

Cite this article as: N. Busom, R. Petrlc, F. Sebé, C. Sorge and M. Valls, A privacy-preserving reputation system with user rewards, *Journal of Network and Computer Applications*, <http://dx.doi.org/10.1016/j.jnca.2016.12.023>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting galley proof before it is published in its final citable form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

A privacy-preserving reputation system with user rewards

N. Busom^{a,*}, R. Petrlc^b, F. Seb[U+00E9]^a, C. Sorge^b, M. Valls^a

^a*Departament de Matem[U+00E0]tica, Universitat de Lleida,
Avda. Jaume II, 69 E-25001 Lleida, Spain*

^b*CISPA, Saarland University, P.O. Box 15 11 50, D-66041 Saarbr[U+00FC]cken, Germany*

Abstract

Reputation systems are useful to assess the trustworthiness of potential transaction partners, but also a potential threat to privacy since rating profiles reveal users' preferences. Anonymous reputation systems resolve this issue, but make it difficult to assess the trustworthiness of a rating. We introduce a privacy-preserving reputation system that enables anonymous ratings while making sure that only authorized users can issue ratings. In addition, ratings can be endorsed by other users. A user who has received a pre-defined number of endorsements can prove this fact, and be rewarded e.g. by receiving a "Premium member" status. The system is based on advanced cryptographic primitives such as Chaum-Pedersen blind signatures, verifiable secret sharing and oblivious transfer.

Keywords: Reputation system, Reputation management, Anonymity, Privacy

1. Introduction

A major difficulty for Internet business in comparison to the traditional economy is the establishment of trust in potential transaction partners. Traditionally, trust has been established by word of mouth, or by surrogates such as

*Corresponding author. Tel.: +34 973 702 774. Fax: +34 973 702 716

Email addresses: nuria@matematica.udl.cat (N. Busom),
ronald.petrlic@uni-saarland.de (R. Petrlc), fsebe@matematica.udl.cat (F.
Seb[U+00E9]), christoph.sorge@uni-saarland.de (C. Sorge), magda@matematica.udl.cat
(M. Valls)

Download English Version:

<https://daneshyari.com/en/article/4956050>

Download Persian Version:

<https://daneshyari.com/article/4956050>

[Daneshyari.com](https://daneshyari.com)