Reputation Management Service for Peer-to-Peer Enterprise Architectures

M. Amoretti, M. Bisi, M.C. Laghi, F. Zanichelli, and G. Conte

Abstract. The high potential of P2P infrastructures for enterprise services and applications both on the intranet (e.g. project workgroups) and on the Internet (e.g. B2B exchange) can be fully achieved provided that robust trust and security management systems are made available.

This paper presents the reputation system we have devised for SP2A [1], a P2P framework which supports secure role-based peergroups and service interactions. Our solution includes decentralized trust and security management able to cope with several threats. The underlying analytical model is introduced and discussed, together with a simulation-based evaluation of the robustness against malicious negative feedbacks.

Keywords: Service Oriented Architectures, Peer-to-Peer, Security, Reputation Management.

1 Introduction

Ubiquitous access to networks is deeply changing the ways enterprises organize and perform their business both internally and externally. Intranets and the global Internet allow for seamless and almost instantaneous information and knowledge sharing within organizations thus enabling more efficient processes and activities and giving rise to novel forms of interaction and supporting applications.

Peer-to-peer (P2P) technologies have gained world-wide popularity due to the success of file-sharing applications (and the predictable reactions of copyright holders) and their decentralized nature appears promising also to the purposes and applications of enterprises. P2P-based instant messaging and file-sharing can be effectively exploited on an intranet to support for example projects workgroups, distributed offices and distributions chains for documents and archives. Internet-enabled inter-firm collaboration can benefit from a P2P approach as well. Business-to-business exchanges are becoming increasingly important and many B2B communities organize themselves to be more competitive in specialized industry sectors by increasing the efficiency of their procurement and supply chains. By leveraging upon P2P technologies, the common tasks of searching for new business partners and exchanging transaction information (e.g. quotations) can be improved in terms of instant information, control over shared data (maintained at each P2P node) and reduced infrastructure costs.
The vision of unmediated, instantaneous trading as well as more realistic P2P-based B2B communities can be approached only if enterprise-level solutions are made available to cope with the fundamental trust and security issues. Identity trust, namely the belief that an entity is what it claims to be, can be assessed by means of an authentication scheme such as X.509 digital identity certificates. Provision trust, that is the relying party’s trust in a service or resource provider, appears more critical as users require protection from malicious or unreliable service providers. Unlike B2B exchanges based on centralized, third party UDDI directories which offer trustworthy data of potential trading partners (i.e. service providers), P2P decentralized interaction lends itself to trust and reputation systems mainly based on first hand experience and second-hand referrals. This information can be combined by a peer into an overall rating or reputation value for a service provider and should influence further interaction with it.

In this paper we present the reputation system we have devised for SP2A [1], a P2P framework which supports secure role-based peergroups and service interactions. Our system includes decentralized trust and security management able to cope with several threats, starting from impersonification, which refers to the threat caused by a malicious peer posing as another in order to misuse that peer’s privileges and reputation. Digital signatures and message authentication are typical solutions for this kind of attack. As malicious peers can engage in fraudulent actions, such as advertising false resources or services and not fulfilling commitments, a consistent reputation management system has been introduced in our P2P framework which also forbids trust misrepresentation attempts. In a peer-to-peer system, the most difficult threat to discover and neutralize is collusion, which refers to a group of malicious peers working in concert to actively subvert the system. To face this danger, the default policy provided by our security framework is role-based group membership based on secure credentials (SC policy). Based on this strategy, a group of peer can filter what actions its members can perform. This paper focuses on reputation management, which was left as open issue in our previous work [2].

Next section 2 outlines the issues of reputation management systems and the choices available for centralized and decentralized implementation. The analytical model underlying our reputation management is described in section 3. An emulation scenario is then presented, first describing a four roles configuration example (section 4) and then discussing the obtained results (section 5). Section 6 reports on some relevant work in the area of reputations systems for P2P systems. Finally, a few conclusive remarks and an indication of further work conclude the paper.

2 Reputation Management in Role-Based Peergroups

A role-based peergroup can achieve stability only if each participant (which is supposed to be authenticated and authorized) bases its actions on previous experience and/or recommendations, i.e. which define the reputation of the other participants. Reputation and trust are orthogonal concepts, which require, in a peer-to-peer context, complex management mechanisms such as node identification and digitally signed certificates exchange [3].