A Requirements-Driven Trust Framework for Secure Interoperation in Open Environments

Suroop Mohan Chandran, Korporn Panyim, and James B.D. Joshi

Department of Information Sciences and Telecommunications,
University of Pittsburgh
smc44@pitt.edu, kop1@pitt.edu, jjoshi@mail.sis.pitt.edu

Abstract. A key challenge in emerging multi-domain open environments is the need to establish trust-based, loosely coupled partnerships between previously unknown domains. An efficient trust framework is essential to facilitate trust negotiation based on the service requirements of the partner domains. While several trust mechanisms have been proposed, none address the issue of integrating the trust mechanisms with the process of integrating access control policies of partner domains to facilitate secure interoperation. In this paper, we propose a requirements-driven trust framework for secure interoperation in open environments. Our framework tightly integrates game-theory based trust negotiation with service negotiation, and policy mapping to ensure secure interoperation.

1 Introduction

In emerging application environments, loosely coupled entities typically collaborate to provide unified solutions. This has led to the development of service-based applications like Web Services, P2P and Grid applications. Business organizations and commercial entities are now moving towards service-based applications to provide integrated solutions with reusable components [21]. The components themselves may be distributed and only Internet-accessible [22]. Typically, services distribution is managed in a centralized manner, either through some service-broker or some public directory [23]. Typically, in such cases, even trust establishment and management is centralized. But with emerging applications, service requirement specification and provision requires a distributed framework. In such cases, recognizing service requirements and composing services that can satisfy these requirements, becomes quite complex. Furthermore, establishing secure interoperation is crucial because of the variety of requirements and the possibility of many domains interoperating in a collaborative framework. Establishment of trust in such environments is the first significant step to establishing secure interoperation. Trust must be negotiated to satisfy the security requirements of all the domains involved. This is done by the disclosure of sensitive information such as credentials, policies, context of service use etc. A trust framework should address all of the above issues.

Several trust negotiation mechanisms have been proposed in the literature including Trust-Serv [1], TrustBuilder [2], H-Trust [4], Trust-X [3] and others [5, 6, 7, 8, 9]. Earlier work has addressed the issue of trust negotiation and trust establishment.
separately. But none of these frameworks have used negotiation and trust computation together. The level of trust to be established is inherently linked to service requirements. These methods fail in the following aspects: (1) primarily based on the client-server interaction model, (2) based on credential exchange and do not handle credential types, and (3) do not consider service requirements as a factor in trust negotiation or establishment.

In this paper, we propose a requirements-based trust framework to support integrated trust and service negotiation, policy mapping, and a ticketing mechanism for fast cross domain accesses. The proposed framework includes the trust sustenance and evolution components. Following are the key contributions of the paper:

- Trust negotiation is driven by service requirements. It supports bi-directional negotiation of service and context requirements.
- Trust negotiation involves establishing agreeable trust levels and trust token types to facilitate mapping of policy elements for secure interoperation. Once negotiation is done, trust tokens are used for authentication and trust tickets are generated to support fast authorized accesses for agreed-upon services under the given context.

The rest of this paper is organized as follows: In section 2, we present related work. In section 3, we present the proposed trust framework. In section 4, the details of service and trust negotiation are presented. In section 5, we discuss the issues behind trust sustenance and evolution and some naïve solutions to the problem.

2 Related Work

The notion of trust among interoperating domains has been loosely divided into two types—negotiation of trust based on credentials and establishing trust based on peer-measured values such as reputation and ranking. Existing work on trust negotiation focuses on the negotiation of credentials, with little focus on the generic requirements of secure interoperation, such as in Trust-Serv [1], TrustBuilder [2], H-Trust [4], Trust-X [3], and others [5, 6, 7, 8, 9]. Trust-Serv is a model-driven framework that uses state machines to represent and determine credential exchanges for access to resources [1]. Both TrustBuilder and Trust-X use credential disclosure trees and negotiation strategies to facilitate protection of credential information during negotiation. TrustBuilder defines families of disclosure trees to facilitate negotiation between entities that have different disclosure trees for the same resource [2]. The Trust-X system introduces the notion of trust ticket for efficient negotiation [3], which has been adopted in our framework.

Decentralized systems typically use trust negotiation based on peer reviews and reputations. HTrust defines functions to establish, sustain and evolve trust based on entity behavior history [4]. Work in [5] defines a trust establishment and sustenance framework for peer to peer systems using reputation as a basis for trust establishment. Reputation is distributed across peers through the formation of peer grids or p-grids. The notion of sustenance is based on the concept of complaints, where peers can