Chapter 6

An Approach to Unified Trust Management Framework

Weiliang Zhao
Macquarie University, Australia

Vijay Varadharajan
Macquarie University, Australia

ABSTRACT

In this chapter, the authors propose an approach with a unified framework for trust management with a consistent way to cover a broad variety of trust mechanisms including credentials, reputation, local data storage, and environment parameters. The trust request, trust evaluation, and trust consuming are handled in a comprehensive manner. The framework has a high extensibility to embrace established standards and new requirements. With the help of the proposed framework, the development of a trust management system in the real world can be automated to a substantially high level.

1. INTRODUCTION

There have been many trust management systems which are exclusively based on credentials. In these systems, credentials are the only type of trust evidence accepted. Before the clear concept of trust management, PKI and PGP have already used credentials to deal with trust management problems. PolicyMaker (Blaze, Feigenbaum, & Lacy, 1996), KeyNote (Blaze, Feigenbaum, & Keromytis, 1999), and REFEREE (Chu, Feigenbaum, LaMacchia, Resnick, & Strauss, 1997) belong to this kind of trust management systems. Normally, these trust management systems include credential verification and security policies to restrict access to resources and services. G. Suryanarayana et al. (Suryanarayana, Erenkrantz, Hendrickson, & Taylor, 2004) have pointed out that these systems are limited in the sense that they do not enable an entity to aggregate the perception of other entities in the system in order to choose a suitable reputable service.

The reputation of an entity can be used as a criterion to determine the restriction of access to resources and services. Some information systems such as e-Bay employ reputation as the exclusive evidence for trust. Reputation-based systems such as XREP (Damiani, Vimercati, Paraboschi, Samarati,
An Approach to Unified Trust Management Framework

& Violante, 2002), NICE (Lee, Sherwood, & Bhattacharjee, 2003), P-Grid (Aberer & Despotovic, 2001) provide the facilities to compute the reputation of an involved entity by aggregating the perception of other entities in the system. Some reputation systems like TrustNet (Schillo, Rovatsos, & Funk, 2000) and NodeRanking (Pujol, Sang, esa, & Delgado, 2002) utilize existing social relationships to compute reputations based on various parameters. M. Kinateder et al (Kinateder, Baschny, & Rothermel, 2005) proposed a generic model for trust based on reputation. Normally, these reputation systems are limited in the sense that they do not link the purpose of reputation to its evaluation.

All existing trust management systems focus on building up a new trust management layer and the concept of trust is normally assumed in a specific context. These systems normally support certain types of trust mechanisms exclusively. Most of them only support credentials or reputation exclusively. We believe that it is necessary to have a unified framework for trust management with the ability to put different trust mechanisms under the same umbrella.

In this chapter, we propose an approach with a unified framework for trust management that can address the above mentioned limitations of current trust management systems. The unified framework uses a consistent way to cover a broad variety of trust mechanisms including credentials, reputation, local data storage, and environment parameters. Different trust mechanisms can be assembled together easily when they are needed. The framework will embrace established standards and existing computing utilities/functions/systems in distributed information systems. A trust management architecture is proposed and the generic computing components in the architecture are described which can be used as enabling tools for the development of sub systems (or a separated layer) for trust management in distributed information systems.

The proposed unified framework for trust management is based on our formal model of trust relationship and unified taxonomy framework of trust proposed in (Zhao, Varadharajan, & Bryan, 2004, 2005b, 2007). The formal model of trust relationship can cover multiple and/or complex trust mechanisms in distributed information systems. The taxonomy framework can reflect the different forms of trust relationships based on their specific characteristics and a range of useful trust relationships can be expressed and compared. We have developed the general methodology for the analysis and modeling of trust relationships in (Zhao, Varadharajan, & Bryan, 2005a, 2006). These research results form a basis of the unified framework for trust management described in this chapter.

For a real trust management system, trust relationships must have been modeled and loaded into the trust management system before these trust relationships are requested by related applications. When a trust relationship is defined, any condition in a condition set must be assessable which means the condition can always be evaluated in the trust management system. The supporting trust mechanisms and condition constraints must be consistently considered in the analysis and modeling of trust relationships and the development of trust management systems. Our concerns in this chapter focus on the general characteristics of trust management systems. The computing components and processes in real systems will be abstracted to generic computing components and processes. We devise TrustEngine as a generic trust management system to express the unified framework. The unified framework for trust management is expressed by TrustEngine with its architecture, generic system components, generic system setting up, and typical operation sequences.

The rest of this chapter is organized as follows. Section 2 highlights major characteristics of trust management issues in distributed information systems. Section 3 provides an overview of our previous research result about unified taxonomy