Chapter V

Holistic Trust Design of E-Services

Stéphane Lo Presti, Royal Holloway, University of London, UK

Michael Butler, University of Southampton, UK

Michael Leuschel, Heinrich-Heine Universität Düsseldorf, Germany

Chris Booth, QinetiQ, UK

Abstract

As a central issue of modern e-services, trust has to be tackled early during the development phases. We present and compare, in this chapter, various works and methodologies that contribute to this aspect. A holistic trust design methodology that combines useful aspects encountered in the existing works is then described in detail. It is based on a systematic analysis of scenarios that describe the typical use of the e-service by using a trust analysis grid. The trust analysis grid is composed of 11 trust issue categories, which cover the various aspects of the concept of trust, and is used to guide the design of the computing system by analyzing and refining the scenarios, and providing hints at the suitability of technologies for the scenario. We illustrate this methodology in several examples.
Introduction

Trust has recently been recognized as a crucial and central property of modern systems that provide e-services in a variety of contexts. Because failing to address this issue correctly may have a profound and costly impact on the e-service development, the issue of trust must be tackled early during the development, so as to identify and mitigate it as early as possible. This chapter covers methodologies that help to do so.

Trust is a human notion that goes beyond technical aspects of the system. It is important that it is not confused with other concepts, for example, security, so that users understand and thus have confidence in the system. This aspect is reinforced by the rapid growth of e-services developed in, for example, pervasive computing (Huangg, Ling, & Ponnekanti, 1999) or multiagent systems (Hanssens, Kulkarni, Tuchinda, & Horton, 2002).

Trust defies traditional analysis in that it encompasses a wide range of other issues at a high level of abstraction, for example, security, risk, social engineering, or the law, in an ever-increasing complex arrangement. The recent literature on trust (see Jøsang, Ismail, & Boyd; Rindeback & Gustavsson, 2004; or Staab, Bhargava, Lilien, Rosenthal, Winslett, & Sloman, 2004, for example) shows a number of ways with which trust can be dealt. But the literature lacks a holistic point of view that can help understand which techniques or technologies are best in various contexts and circumstances.

The design phase of the system development is the most appropriate time for analysis of trust in the system. This is the approach used to tackle more traditional issues like risk (Storey, 1996) and security (Anderson, 2001), and it has proven successful in improving the quality of systems. It can be seen as a process whose output is a set of requirements that must be addressed in the subsequent phases of the development.

Based on those two ideas of holistic design, trust is considered, in this chapter, as an evolving, contextual, and composite belief that one principal (trustor) has that another principal (trustee) will perform certain actions with certain expected results, when not all information about those actions is available. The various elements of this definition will be detailed in the remainder of this chapter.

The first section presents current works on methodologies to help design trustworthy e-services. Then we present a methodology that builds upon the current understanding of trust and improves on the existing trust design methodologies. It provides a holistic analysis framework to help design trustworthy e-services where the user is the focus of attention. This framework is applied to several realistic systems under development, including e-health and e-learning, in the next section.

Existing Methodological Work

Tackling the Trust Issue

There is a huge corpus of work on the issue of trust, but few concentrate on this issue during the design of a system development, and fewer propose methodologies to help the
Related Content


Securing Data Storage By Extending Role-Based Access Control
[www.igi-global.com/article/securing-data-storage-by-extending-role-based-access-control/105508?camid=4v1a](www.igi-global.com/article/securing-data-storage-by-extending-role-based-access-control/105508?camid=4v1a)

Web Services, Service-Oriented Computing, and Service-Oriented Architecture: Separating Hype from Reality
[www.igi-global.com/chapter/web-services-service-oriented-computing/43942?camid=4v1a](www.igi-global.com/chapter/web-services-service-oriented-computing/43942?camid=4v1a)
Ranking Model for SLA Resource Provisioning Management
[www.igi-global.com/article/ranking-model-for-sla-resource-provisioning-management/120247?camid=4v1a](www.igi-global.com/article/ranking-model-for-sla-resource-provisioning-management/120247?camid=4v1a)