

Design of a Trust Model for a Secure Multi-Agent Marketplace

S. Robles, J. Borrell
Departament d'Informàtica
Universitat Autònoma de Barcelona
08193 Bellaterra - Spain
+34 93 5812395

Sergi.Robles@uab.es

J. Bigham, L. Tokarchuk, L. Cuthbert
Dept of Electronic Engineering
Queen Mary, University of London
Mile End Road, London E1 4NS - UK
+44 20 7882 5350

J.Bigham@elec.qmw.ac.uk

ABSTRACT

A general trust model and security framework for a multi-agent system designed to manage resources in future mobile communications networks is described. The multi-agent system is being developed as part of the IST SHUFFLE project [1]. A business model appropriate for selling of bandwidth resource and services is investigated and mechanisms to achieve a Global Trust Model is outlined. Our trust model for the marketplace is based on concentric spheres structure. The core of this model will be physical security. A security infrastructure is located in middle spheres: the internal and the external security infrastructure. In outer spheres we will use complex aspects of trust such as fairness, reliability, reputation and loyalty to provide a complete model of basic trust for marketplaces.

Keywords

Artificial Market Systems & e-Commerce, Privacy and Agents, Real-Time Performance, Trust Model

1. INTRODUCTION

The use of agent systems to support the management of resources in telecommunications networks was first investigated in the IMPACT and FACTS projects [4]. The former successfully demonstrated the use of agents to perform real time connections to an ATM network in the context of multiple service providers and user specified (explicitly or implicitly) QoS requirements. Security issues associated with the IMPACT business model have been addressed in [2]. However, the business models associated with managing future mobile communications networks raise other issues and these are the subject of this paper. A model for the creation of a secure marketplace for bandwidth transactions is outlined, and how this generalises to service oriented transactions in a generic marketplace is indicated. The marketplace, as described, is in itself a multi-agent system providing a secure e-trading and e-commerce centre oriented to business to business activities.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

AGENTS'01, May 28-June 1, 2001, Montréal, Québec, Canada.
Copyright 2001 ACM 1-58113-326-X/01/0005...\$5.00.

The resource management system can be viewed as three layers, namely the facilities layer, the negotiation layer and the resource layer.

2. MARKETPLACE

The purpose of this section is to briefly describe a non-discriminatory, secure environment in which an multi-agent system could operate. This system, which we call the marketplace exists to provide a secure trading environment in which agents may trade. In our example of the marketplace, the commodity being traded is bandwidth.

2.1 Business Environment

As in any business arrangement, each party has its' own interests in mind. Resources (typically bandwidth) are provided by Network Providers (NPs) who own the physical network. The resources are sold to customers through Service Providers (SPs). A Network Provider may also act as a Service Provider in its own right. Such a SP is much like any other but, depending upon regulatory constraints, may have more control options than other SPs. The liberalisation of telecommunications networks is expected to lead to an "any-to-any" scenario with any customer being free to buy services from any SP, who in turn could buy network capacity from any NP. SP to SP exchange is also possible. This has the advantage of allowing SPs to offload excess bandwidth to others who may want it and another way to buy bandwidth other than directly through a NP.

2.2 Marketplace Model

The introduction of agents goes beyond the interaction between the customer and the service provider. As shown by the European Union ACTS projects IMPACT and FACTS, there is a significant role for agents to play in managing the resources within and between SPs and NPs. Combining the control of the resources of both the SP and the NP leads us to propose an outline three layer marketplace architecture:

- The **facilities plane** houses the entities that ensure secure interactions in the negotiation plane. Confidence (as determined by the facilities provided) is an important concept at this level. Facilities are provided to allow the agents in the negotiation plane to participate in indirect trading relationships, such as blind auctions, as well as infrastructure services.
- The **negotiation plane** is where all interaction between the customers, the SPs and the NPs takes place. In this plane the service provider winning the business sets up the connection

using a network operator of its choosing. Reputation and the maintenance of statistics for measuring reputation is an important concept at this level to provide fast decision making.

- The **resource plane** is where the network operator manages its resources both across and within individual radio cells. Reliability and survivability are important operational considerations at this level..

Splitting the system into these three make different services to be more independent, providing flexibility (as behavior of services may change), and adaptability (new services can be added without modifying the design).

2.3 Trust model

Marketplaces in highly competitive business models should be based on a strong trust model. Trust is recognized by many to be cardinal to information security, security policies, accountability, reliability, business relationships, etc. At this time, there are no satisfactory answers as to what trust is, no consensus and no well-defined models. However, some references related to trust theory show some results linked to cryptography and certification. The trust model we use, will allow us to represent our understanding of the word "trust" not only in reference to the trust between agent entities, but also "trust" in regards to the system itself.

Our trust model for the marketplace is based on a concentric spheres structure. The core of this onion-like model will be physical security and it is assumed that this is provided. A security infrastructure is located in middle spheres: the internal and the external security infrastructure. In outer spheres we will use complex aspects of trust such as fairness, reliability, reputation or loyalty to provide a complete model of basic trust for marketplaces. Figure 1 shows a synoptic cube of the trust model.

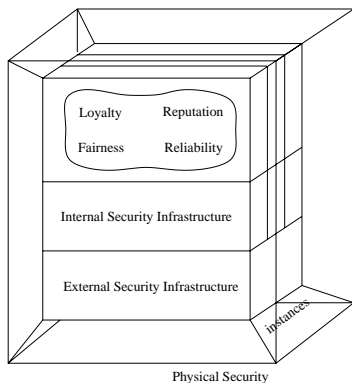


Figure 1. Trust Model

The inner sphere of the trust model is the external security infrastructure. This infrastructure is useful in multi-instanced marketplaces. It is based on a Public Key Infrastructure (PKI), a well-known security infrastructure with many security protocols are designed for it [3].

The external security infrastructure will provide coherence, integrity and trust to a multi-instanced marketplace. A party submitting its agent to the marketplace has to be confident that the agent is not going to be cheated in the marketplace, but also that the integrity of the agent will persist in all the instances of the marketplace. The solution to this problem is to have a simple PKI

to keep the cohesion, in terms of trust, of the marketplace. In the particular scenario we are managing, the telecommunications regulatory body (e.g. Ofel in the UK) is the trusted third party.

2.3.2 Internal Security Infrastructure

Every instance of the marketplace has its own internal security infrastructure. A Public Key Infrastructure (PKI) like the one presented in the previous section is also used here. As a requirement, the keys of the internal PKI used in every instance must be unknown to the external security infrastructure. This avoids the owner of the marketplace controlling (read cheating) specific instances. This is an added feature of this model of the marketplace with instances comparing to the unique marketplace approach: if the marketplace code is accepted all instances are trustworthy since they control themselves with private PKIs.

2.3.3 High level trust

In the top layers of the trust model, more complex and high level concepts of trust are managed. These concepts are described in sections about the marketplace architecture. The main aspects include reputation, loyalty, reliability, fairness and confidence.

Some of these aspects are related to different layers of the marketplace. For example, the concept of reliability is linked with the resource plane, while reputation or loyalty are linked with the negotiation plane.

3. ACKNOWLEDGMENTS

Contributions of S. Robles and J. Borrell have been partially funded by the Spanish Government Commission CICYT, through its grant TIC2000-0739-C04-01.

4. CONCLUSIONS

A trust model for a multi-agent marketplace has been presented. We have analyzed a business environment for selling of bandwidth resource and services.

The trust model is based on concentric spheres structure, with physical security in the core, a security infrastructure in middle spheres and complex aspects of trust in outer spheres, such as reputation, fairness and reliability. Benefits of the partition of the trust model into shells are adaptability, flexibility and scalability. For example, it is very easy to add new facilities or norms or use the model in a large scale marketplace.

5. REFERENCES

- [1] Shuffle project URL: <http://www.ist-shuffle.org>
- [2] Bigham, J., Cuthbert, L., Hayzelden, A., Borrell, J., and Robles, S. Distributed Control of Connection Admission to a Telecommunications Network: Security Issues. In Proceedings of the 4th World Multiconference on Systemics, Cybernetics and Informatics, Orlando, Florida, 2000, pp224-229, Vol VII, Computer Science and Engineering Part 1. ISBN 980-07-6693-6
- [3] Scheneier, B. Applied Cryptography. Protocols, Algorithms, and Source Code in C. John Wiley & Sons, New York, 1996.
- [4] Agent Technology for Communications Infrastructure, John Wiley, (being published) , Editors Hayzelden, A.L.G. and Bourne, R.