Available online at www.sciencedirect.com
SCIENCE DIRECT®
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 157 (2006) 43–59
www.elsevier.com/locate/entcs

Application Security Models for Mobile Agent Systems

J. Todd McDonald[1]

Department of Computer Science
Florida State University
Tallahassee, FL, USA

Alec Yasinsac[2]

Department of Computer Science
Florida State University
Tallahassee, FL, USA

Abstract

Mobile agents are a distributed computing paradigm based on mobile autonomous programs. Mobile applications must balance security requirements with available security mechanisms in order to meet application level security goals. We introduce a trust framework to reason about application security requirements, trust expression, and agent protection mechanisms. We develop application security models that capture initial trust relationships and consider their use for mobile agent security.

Keywords: Mobile agents, trust, security, application requirements, software protection, models, frameworks

[1] Email:mcdonald@cs.fsu.edu. The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government

[2] Email: yasinsac@cs.fsu.edu. This material is based upon work supported in part by the U.S. Army Research Laboratory and the U.S. Army Research Office under grant number DAAD19-02-1-0235

doi:10.1016/j.entcs.2005.09.041

1 Introduction

Mobile agents are autonomous programs with the capability of changing their execution location through a series of migrations and corresponding state updates. Mobile agent applications specify and enforce security requirements based on the unique interactions of agent servers (hosts) with static and dynamic agent components.

Traditionally, mobile agent security has focused on two forms of protection: keeping malicious parties from altering the agent and keeping malicious agents from harming other parties including potential hosts. Several surveys [1,2,3] categorize and describe attacks against agent systems along with mechanisms for defense.

Trust formulation has been given considerable thought both in distributed networking applications [4,5,6,7] and mobile agents [8,9,10,11,12]. Mobility as an application feature complicates trust because the receiving execution host must make distributed trust decisions in the face of little or no prior knowledge. Likewise, user agents must evaluate trust with hosts in different security contexts.

To date, other trust models for mobile agents have not addressed how to link requirements with appropriate agent protection mechanisms. Other trust models lack integration of generic security mechanisms or reasoning about initial trust relationships (what we term an *application security model*). We bridge this gap by posing a trust-based security framework for mobile agents with three novel features:

- Ability to link application security requirements with mechanisms based on trust
- Reasoning about trust properties for generic security mechanisms
- Application models for initial trust among principals in a mobile agent setting

The rest of this paper describes our trust framework and is organized as follows: section 2 discusses related works concerning trust and security requirements in the mobile agent paradigm. Section 3 presents our framework for expressing trust and security in mobile agent systems. Section 4 expounds three different application-level security models and section 5 summarizes our contributions.