IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB8583

Chapter XX

Intelligent Mobile Agents for E-Commerce: Security Issues and Agent Transport

Yang Yang and Sheng-Uei Guan
National University of Singapore

INTRODUCTION

With the proliferation of Internet, electronic commerce (e-commerce) is beginning to take the center stage in the commerce world. Transactions via electronic means have been growing rapidly over recent years, both in terms of turnover amount and volume. It is estimated that the trend will continue, as more and more businesses have already started or have plans to put their products/services online.

However, the development of e-commerce is hindered by several factors. One of them is the lack of intelligence. Today, there is little intelligence in the World Wide Web. Users cannot delegate jobs to 'agents' that autonomously perform the desired tasks for their owners. One way to resolve this is through the introduction of 'smart software programs', or intelligent agents. With an agent architecture in place, users can delegate tasks to agents. An agent can help its owner to search for and filter information, negotiate with other agents, and even perform transactions on behalf of its owner. It is predicted that agent usage will become the mainstream in the future, not just in the field of e-commerce, but in the World Wide Web as well (Guilfoyle, 1994; Corley, 1995).

Due to the nature of e-commerce, security becomes a primary concern for any architecture under this category. In fact, the threats to e-commerce come mostly from the area of security. Credit card companies lose billions of dollars every year on card frauds. Bank networks are broken into and millions are transferred out without the administration's immediate knowledge. In order to fight against these electronic crimes, it is necessary to protect our architecture with a solid security framework.

Besides the security needs, it is desirable for agents to have roaming capability as well. Roaming extends the agent's capability well beyond the limitations imposed by its owner's computer. Agent operations should not be affected by factors such as the availability of network, the limitation on bandwidth, or the lack of computing resources. Roaming agents should be able to physically leave their owners' machines and perform their operations using the computing resources on hosting machines.

In view of the various needs above, SAFE (**S**ecure-roaming **A**gent **F**or **E**-commerce), an agent architecture covering on security and roaming capability, is being developed for e-commerce applications. One of the core elements in SAFE is the agent transport protocol, which allows intelligent agents to roam from one host to another in a secure fashion.

SAFE aims to provide a framework for the development of intelligent agent systems, so as to facilitate intelligent agents' roaming from hosts to hosts to fulfill electronic commerce-related missions. As will be discussed in this chapter, security issues incurred from roaming agents and related agent transport protocol lay a secure foundation for mobile agents. With its powerful roaming capability and strong security feature, SAFE is suitable for use as a middleware layer in the next generation of e-commerce applications.

BACKGROUND

Intelligent agent is not a new area of research. Over the years, there has been a lot of research on intelligent agents, resulting in various agent systems being proposed. Efforts on standardization are also under way to establish a universal basis for intelligent agent development. One of the most widely accepted standards is KQML (Finin, 1993; 1994) (Knowledge Query and Manipulation Language), developed as part of the *Knowledge Sharing Effort*. Despite being a high level language for run-time exchange of information between heterogeneous systems, KQML is not designed with security in mind as there is no security mechanism built in KQML to address the common security concerns, not to mention those introduced by roaming. Agents using KQML still need to implement their own security mechanism to protect themselves. Secret Agent (Thirunavukkarasu, 1995) is one of the security architectures designed for to fill in the gap for KQML.

Secret Agent provides a security layer for agents systems using KQML. However, it has a number of shortcomings and is restricted by the nature of KQML. Firstly, Secret Agent requires every agent that implements the security algorithm to possess a key (master key). If the key is based on a symmetric key algorithm, the authors suggest every agent have additional master keys for each agent that it wishes to communicate with. The prerequisite for an agent to communicate with another is that both of them have the knowledge of a common master key, which is exclusive to the two of them. This requirement may restrict the agent's capability and efficiency if it wishes to communicate with many other agents. At the same time, the maintenance as well as protection of the master key database may pose additional security threats to agent systems. For example, if the key database of agent 007 is compromised, all agents corresponding with agent 007 will be compromised. The point of failure is at every agent's database, which is highly undesirable in the field of security.

Furthermore, if the agent intends to talk to an agent with whom it has no common master key, a central authentication server is required to generate such a key. The use of a central authentication server introduces many issues into the architecture. Among them are potential attacks on the authentication server, key transport/exchange algorithm, key database management etc.

If the master key is based on a public key algorithm, the agent identity must be tightly tied to the key pair. This was not carefully addressed in the Secret Agent design, subjecting the algorithm to man-in-the-middle attack. For example, when agent A and B start a handshake, if a third agent C can intercept all messages between A and B, agent C can pretend to be agent A while talking to agent B, and pretend to be agent B while talking to