Chapter XLII
Roaming-Agent Protection for E-Commerce

Sheng-Uei Guan
Brunel University, UK

INTRODUCTION

There has been a lot of research done in the area of intelligent agents. Some of the literature (Guilfoyle, 1994; Johansen, Marzullo, & Lauvset, 1999) only proposes certain features of intelligent agents, while some of it attempts to define a complete agent architecture. Unfortunately, there is no standardization in the various proposals, resulting in vastly different agent systems. Efforts are being made to standardize some aspects of agent systems so that different systems can interoperate with each other.

Knowledge representation and exchange is one of the aspects of agent systems for which KQML (knowledge query and manipulation language; Finin & Weber, 1993) is one of the most widely accepted standards. Developed as part of the knowledge sharing effort, KQML is designed as a high-level language for run-time exchange of information between heterogeneous systems. Unfortunately, KQML is designed with little security considerations because no security mechanism is built to address common security concerns, not to mention specific security concerns introduced by mobile agents. Agent systems using KQML will have to implement security mechanisms on top of KQML to protect themselves.

While KQML acts as a sufficient standard for agent representation, it does not touch upon the security aspects of agents. In an attempt to equip KQML with built-in security mechanisms, Secret Agent is proposed by Thirunavukkarasu, Finin, and Mayfield (1995).

Another prominent transportable agent system is Agent TCL developed at Dartmouth College (Gray, 1997; Kotz, Gray, Nog, Rus, Chawla, & Cybenko, 1997). Agent TCL addresses most areas of agent transport by providing a complete suite of solutions. It is probably one of the most complete agent systems under research. Its security mechanism aims at protecting resources and the agent itself. In terms of agent protection, the author acknowledges that "it is clear that it is impossible to protect an agent from the machine on which the agent is executing…it is equally clear that it is impossible to protect an agent from a resource that willfully provides false information" (Gray). As a result, the author "seeks to implement a verification mechanism so that each machine can check

whether an agent was modified unexpectedly after it left the home machine" (Gray). The other areas of security, like nonrepudiation, verification, and identification, are not carefully addressed.

Compared with the various agent systems discussed above, the SAFE (secure roaming agent for e-commerce) transport protocol is designed to provide a secure agent roaming mechanism for e- or m-commerce. The other mobile agent systems are either too general or too specific to a particular application. By designing SAFE with mobile application concerns in mind, the architecture will be suitable for m-commerce. The most important concern is security as discussed previously. Due to the nature of m-commerce, security becomes a prerequisite for any successful m-commerce application. Other concerns are mobility, efficiency, and interoperability. In addition, the design allows certain flexibility to cater to different application needs.

BACKGROUND

The introduction of the mobile Internet is probably one of the most significant revolutions of the 20th century. With a simple click, one can connect to almost every corner of the world thousands of kilometers away. This presents a great opportunity for m-commerce. Despite its many advantages over traditional commerce, m-commerce has not taken off successfully. One of the major hindrances is that of security. The focus of this chapter is the secure transport of mobile agents. A mobile agent is useful for handheld devices like palmtops or PDAs (personal digital assistants). Such m-commerce devices usually have limited computing power. It would be useful if the users of such devices can send an intelligent mobile agent to remote machines to carry out complex tasks like product brokering, bargain hunting, and information collection.

When it comes to online transactions, security becomes the primary concern. The Internet was developed without too much security in mind. Information flows from hub to hub before it reaches the destination. By simply tapping into wires or hubs, one can easily monitor all traffic transmitted. For example, when Alice uses her Visa credit card to purchase an album from Virtual CD Mall, the information about her card may be stolen if it is not carefully protected. This information may be used maliciously to make other online transactions, thus causing damage to both the card holder and the credit card company.

Besides concerns of security, current m-commerce lacks the intelligence to locate the correct piece of information. The Internet is like the world's most complete library collection unsorted by any means. To make things worse, there is no competent librarian that can help readers locate the book wanted. Existing popular search engines are attempts to provide librarian assistance. However, as the collection of information is huge, none of the librarians are competent enough at the moment.

The use of intelligent agents is one solution for providing intelligence in m-commerce. However, having an agent that is intelligent is insufficient. There are certain tasks that are unrealistic for agents to perform locally, especially those that require a huge amount of information. Therefore, it is important to equip intelligent agents with roaming capability.

Unfortunately, with the introduction of roaming capability, more security issues arise. As the agent needs to move among external hosts to perform its tasks, the agent itself becomes a target of attack. The data collected by agents may be modified, the credit carried by agents may be stolen, and the mission statement on the agent may be changed. As a result, transport security is an immediate concern to agent roaming.

Agent Protection

SAFE is a protocol designed to provide a secure roaming mechanism for intelligent agents.