Chapter 7.3
Security in Mobile Agent Systems

Chua Fang Fang
Multimedia University, Malaysia

G. Radhamani
Multimedia University, Malaysia

ABSTRACT

Agent technologies have grown rapidly in recent years as Internet usage has increased tremendously. Despite its numerous practical benefits and promises to provide an efficient way of mitigating complex distributed problems, mobile agent technology still lacks effective security measures, which severely restricts its scope of applicability. This chapter analyzes and synthesizes the different security threats and attacks that can possibly be imposed to mobile agent systems. The security solutions to resolve the problems and the research challenges in this field are presented.

INTRODUCTION

Software agent is a very generic term for a piece of software that can operate autonomously and that helps facilitate a certain task. Software agents can communicate and be intelligent in the way that they have the attributes of proactive/reactive, and have learning capabilities. In agent-based systems, humans delegate some of their decision-making processes to programs that are intelligent, mobile, or both (Harrison, Chess, & Kershenbaum, 1995). Software agents may be either stationary or mobile, such that stationary agents remain resident at a single platform while mobile agents are capable of suspending activity on one platform and moving to another, where they resume execution (Jansen, 2000). In most mobile intelligent agent systems, the software agent travels autonomously within the agent-enabled networks, executes itself in the agent execution environment, gathers related information, and makes its own decision on behalf of its owner.

SCOPE

Currently, distributed systems employ models in which processes are statically attached to hosts and communicate by asynchronous messages or synchronous remote procedure calls; mobile agent technology extends this model by including mobile processes (Farmer, Guttman, & Swarup, 1996a). Compared to the client/server model, the mobile agent paradigm offers great opportunities for performing various attacks because mobile agent systems provide a distributed computing infrastructure where applications belonging to different users can execute concurrently (Bellavista, Corradi, Federici, Montanari, & Tibaldi, 2003).

A mobile agent is an object that can migrate autonomously in a distributed system to perform tasks on behalf of its creator. It has the ability to move computations across the nodes of a wide-area network, which helps to achieve the deployment of services and applications in a more flexible, dynamic, and customizable way than the traditional client-server paradigm. For instance, if one needs to perform a specialized search of a large free-text database, it may be more efficient to move the program to the database server than to move large amounts of data to the client program. Security issues in regard to the protection of host resources, as well as the agent themselves, are extremely critical in such an environment. Apart from that, there is a greater chance for abuse or misuse, and it is difficult to identify a particular mobile process with a particular known principal and to depend on the reference monitor approach to enforce the security policy (Varadharajan, 2000).

PROBLEM STATEMENT

The general lack of security measures in existing mobile intelligent agent systems restricts their scope of applicability. According to Bellavista et al. (2003), the widespread acceptance and adoption of the mobile agent technology is currently delayed by several complex security problems that still need to be completely solved. Harrison et al. (1995) identifies security as a severe concern and regards it as the primary obstacle in adopting the mobile agent systems. Full-scale adoption of mobile agent technology in untrustworthy network environments, for example Internet, has been delayed by several security complexities. The security risks that can be encountered in mobile agent environments include malicious hosts, malicious agents, and malicious network entities. Without an appropriate security level for agents, mobile agent applications could only execute in trusted environments, and could not be deployed in the Internet scenario.

To illustrate the security requirements and issues raised by the mobile agent technology (Bellavista et al., 2003), consider the case of a shopping mobile agent that has to find the most convenient offer for a flight ticket. Suppose that Babu accesses a flight-ticket booking service (FBS) to search for and book the cheapest Rome-to-London flight ticket. Before starting an FBS provisioning session, the client requires Babu to authenticate. After a successful authentication, a middleware mobile proxy called Alfred is instantiated to represent Babu over the fixed network and to support Babu's shopping operations. A trusting relationship should be established between Babu and Alfred now that Alfred generates a shopping mobile agent and delegates it the flight searching and booking operations. The shopping agent could migrate among the various air-travel agencies' nodes to locally operate on needed resources. Once its tasks are completed, the shopping agent should be granted the same rights and submitted to the same restrictions as Alfred. In this scenario, several security issues arise and several attacks such as user-agent trust, interagent security, agent-node security, and so forth, are possible, as Figure 1 shows.