Chapter 8
Securing Mobile-Agent Systems through Collaboration

Mohammed Hussain  
Queen’s University, Canada

David B. Skillicorn  
Queen’s University, Canada

ABSTRACT
Mobile agents are self-contained programs that migrate among computing devices to achieve tasks on behalf of users. Autonomous and mobile agents make it easier to develop complex distributed systems. Many applications can benefit greatly from employing mobile agents, especially e-commerce. For instance, mobile agents can travel from one e-shop to another, collecting offers based on customers’ preferences. Mobile agents have been used to develop systems for telecommunication networks, monitoring, information retrieval, and parallel computing. Characteristics of mobile agents, however, introduce new security issues which require carefully designed solutions. On the one hand, malicious agents may violate privacy, attack integrity, and monopolize hosts’ resources. On the other hand, malicious hosts may manipulate agents’ memory, return wrong results from system calls, and deny access to necessary resources. This has motivated research focused on devising techniques to address the security of mobile-agent systems. This chapter surveys the techniques securing mobile-agent systems. The survey categorizes the techniques based on the degree of collaboration used to achieve security. This categorization resembles the difference between this chapter and other surveys in the literature where categorization is on the basis of entities/parts protected and underlying methodologies used for protection. This survey shows the importance of collaboration in enhancing security and discusses its implications and challenges.

INTRODUCTION
The concept of software agents originated in the artificial intelligence field as a paradigm for software design and development (Jennings & Wooldridge, 1998). Software agents have received attention in the distributed systems field, mainly because mobile agents add mobility to agency. A mobile-agent system (MAS) consists of a set of computing devices, called hosts, and autonomous programs
called agents. Users of such a system encapsulate their tasks in agents. The agents then roam the hosts, hence the word mobile, finding and utilizing resources and information needed to accomplish their goals (Pham & Karmouch, 1998). The set of hosts visited by a mobile agent is its itinerary. Examples of mobile-agent frameworks include Telescript (White, 1994), JADE (Bellifemine, Caire, Poggi, & Rimassa, 2003), D’Agents (Gray, Cybenko, Kotz, Peterson & Rus, 2002), Aglet (Lange & Oshima, 1998), Concordia (Castillo, Kawaguchi, Paciorek & Wong, 1998), Voyager (Recursion Software, 2006), and Spider (Huang & Skillicorn, 2001).

Mobile agents combine software agency from artificial intelligence and software mobility from distributed systems. Advantages are inherited from both areas. Although mobile agents have no major application justifying their usage so far, their benefits have been suggested by many studies (Das, Shuster, Wu & Levit, 2005; Ghanea-Hercock, Collis & Ndumu, 1999; Guttman, Moukas & Maes, 1998; Maes, Guttman & Moukas, 1999). Mobile agents can:

- Reduce network traffic significantly by moving agents to where data resides rather than moving data to users.
- Perform their tasks when their owner is offline, a valuable feature when network connections cannot be sustained during an entire task execution.
- Facilitate parallel computing by utilizing groups of hosts.
- Execute on heterogeneous environments and adapt to changes.

E-commerce, parallel computing, information retrieval, and monitoring are a few applications for which mobile agents can be of a great help. Mobile agents can search for related products based on a consumer needs, compare offers from different merchants, and choose products that best fit the consumer criteria. In (Guttman et al., 1998) the automation of different stages of consumer buying behavior using mobile agents is studied. Telecommunication networks can utilize mobile agents to reconfigure networks and machines (sending an agent instead of sending a technician). Load balancing is another candidate task for mobile agents in telecommunication networks. Mobile agents are employed for a distributed and heterogeneous information retrieval system in (Das et al., 2005). Monitoring applications, especially distributed intrusion-detection systems, can also benefit from using mobile agents.

Industrial applications employing mobile agents, however, have not yet become mainstream. Lack of standards for mobile-agent platforms and challenging security problems are the main barriers to widespread adoption of this technology (Borselius, 2002; Vigna, 2004; Zachary, 2003). Malicious agents may consume hosts’ resources, read private data, modify files, or use a host as a base to send spam. On the other hand, hosts have full control over mobile agents. Malicious hosts may deprive agents of resources, read or modify private data, masquerade as another host, supply illegal input, or re-execute the agent to reverse engineer it (Zachary, 2003). This has motivated research focused on devising techniques to address the security of MAS. These techniques vary in: the parts of systems being protected, the level of protection, and the cost of protection.

This chapter surveys the field of mobile-agent security. Techniques in this field are categorized on the basis of utilizing collaboration. The rationale behind this categorization is to emphasize the importance of collaborative security in the context of MAS. The benefits and costs associated with collaboration are also discussed. Previous surveys (Bellavista, Corradi, Federici, Montanari & Tibaldi, 2004; Borselius, 2002; Claessens, Preneel & Vandewalle, 2003; Jansen & Karygiannis, 2000; Pleisch & Schiper, 2004) focus on comparing the techniques based on entities protected and underlying methodologies used for protection.