Chapter III
Security of Mobile Code

Zbigniew Kotulski
Polish Academy of Sciences, Warsaw, Poland
Warsaw University of Technology, Poland

Aneta Zwierko
Warsaw University of Technology, Poland

ABSTRACT

The recent development in the mobile technology (mobile phones, middleware, wireless networks, etc.) created a need for new methods of protecting the code transmitted through the network. The oldest and the simplest mechanisms concentrate more on integrity of the code itself and on the detection of unauthorized manipulation. The newer solutions not only secure the compiled program, but also the data, that can be gathered during its "journey," and even the execution state. Some other approaches are based on prevention rather than detection. In this chapter we present a new idea of securing mobile agents. The proposed method protects all components of an agent: the code, the data, and the execution state. The proposal is based on a zero-knowledge proof system and a secure secret sharing scheme, two powerful cryptographic primitives. Next, the chapter includes security analysis of the new method and its comparison to other currently more widespread solutions. Finally, we propose a new direction of securing mobile agents by straightening the methods of protecting integrity of the mobile code with risk analysis and a reputation system that helps avoiding a high-risk behavior.

INTRODUCTION

A software agent is a program that can exercise an individual's or organization's authority, work autonomously toward a goal, and meet and interact with other agents (Jansen & Karygiannis, 1999). Agents can interact with each other to negotiate contracts and services, participate in auctions, or barter. Multi-agent systems have sophisticated applications, for example, as management systems for telecommunication networks or as artificial intelligence (AI)-based intrusion detection systems. Agents are commonly divided into two types:

- Stationary agents
- Mobile agents

The stationary agent resides at a single platform (host), the mobile one can move among different platforms (hosts) at different times.

The mobile agent systems offer new possibilities for the e-commerce applications: creating new types of electronic ventures from e-shops and e-auctions to virtual enterprises and e-marketplaces. Utilizing the agent system helps to automate many e-commerce tasks. Beyond simple information gathering tasks, mobile agents can take over all tasks of commercial transactions, namely, price negotiation, contract signing, and delivery of (electronic) goods and services. Such systems are developed for diverse business areas, for example, contract negotiations, service brokering, stock trading, and many others (Corradi, Cremonini, Montanari, & Stefanelli, 1999; Jansen & Karygiannis, 1999; Kulesza & Kotulski, 2003). Mobile agents can also be utilized in code-on-demand applications (Wang, Guan, & Chan, 2002). Mobile agent systems have advantages even over grid computing environments:

- Require less network bandwidth
- Increase asynchrony among clients and servers
- Dynamically update server interfaces
- Introduce concurrency

The benefits from utilizing the mobile agents in various business areas are great. However, this technology brings some serious security risks; one of the most important is the possibility of tampering with an agent. In mobile agent systems the agent's code and internal data autonomously migrate between hosts and can be easily changed during the transmission or at a malicious host site. The agent cannot itself prevent this, but different countermeasures can be utilized in order to detect any manipulation made by an unauthorized party. They can be integrated directly into the agent system, or only into the design of an agent to extend the capabilities of the underlying agent system.

Several degrees of agent's mobility exist, corresponding to possibilities of relocating code and state information, including the values of instance variables, the program counter, execution stack, and so forth. The mobile agent technologies can be divided in to two groups:

- **Weakly mobile:** Only the code is migrating; no execution state is sent along with an agent program
- **Strong mobile:** A running program is moving to another execution location (along with its particular state)

The protection of the integrity of the mobile agent is the most crucial requirement for the agent system. The agent's code and internal data autonomously migrate between hosts and can be easily changed during the transmission or at a malicious host site. A malicious platform may make subtle changes in the execution flow of the agent's code; thus, the changes in the computed results are difficult to detect. The agent cannot itself prevent this, but different countermeasures can be utilized in order to detect any manipulation made by an unauthorized party. They can be integrated directly into the agent system, or only into the design of an agent to extend the capabilities of the underlying agent system. However, the balance between the security level and solution implementation's cost, as well as performance impact, has to be preserved. Sometimes, some restrictions of agent's mobility may be necessary.

Accountability is also essential for the proper functioning of the agent system and establishing trust between the parties. Even an authenticated agent is still able to exhibit malicious behavior to the platform if such a behavior cannot later be detected and proved. Accountability is usually realized by maintaining an audit log of security-relevant events. Those logs must be protected from unauthorized access and modification. Also the non-repudiability of logs is a huge concern. An important factor of accountability is authentication. Agents must be able to authenticate to platforms and other agents and vice versa. An agent may require different degrees of authentication depending on the level of sensitivity of the data.

The accountability requirement needs also to be balanced with an agent's need for privacy. The platform may be able to keep the agent's identity secret from other agents and still maintain a form of revocable anonymity where it can determine the agent's identity if necessary and legal. The