Distributed Object and Mobile Code Security

Vipin Swarup
The MITRE Corporation
Bedford, MA 01730
E-mail: swarup@mitre.org

March 11, 1996

Currently, distributed systems employ models in which processes are statically attached to hosts and communicate by asynchronous messages or synchronous remote procedure calls. Threats, vulnerabilities, and countermeasures for these systems have been studied extensively and sophisticated distributed system security architectures have been designed. Recent work on secure network objects and the Theta and Spring object-oriented operating systems address the need to provide security for object-oriented network communication.

Mobile agent technology extends this model by including mobile processes, i.e., processes which can autonomously migrate to new hosts. Although numerous benefits are expected, this extension results in new security threats from malicious agents and hosts. The primary added complication is that, as an agent traverses multiple machines that are trusted to different degrees, its state can change in ways that adversely impact its functionality.

Several security goals for mobile agent systems appear impossible to achieve. For instance, there appears to be no uniform and reliable way to authenticate interpreters, to ensure that interpreters will run agents correctly, to keep the code and data of agents private, or to have agents carry their own keys. Other goals are achievable using familiar techniques for distributed system security. For instance, an interpreter can authenticate the author and sender of an agent, check the integrity of an agent's code, ensure agent privacy during transmission, and protect itself against agents. Yet other goals appear achievable with the development of special techniques. For instance, special techniques are needed to permit a sender to restrict the authority of his agents in a flexible manner or to enable an interpreter to check that an agent is in a safe state.

We are currently developing a mobile agent security architecture that extends an existing distributed system security architecture with special mechanisms that provide security in the presence of migrating stateful agents. Our emphasis is on agents written by known software developers and our architecture will protect both agent-based distributed systems and the hosts that support them. Since many significant applications require mobile agents to interact with remote network objects, our work seeks to integrate the security services of object-based and web-based technologies. Our position is that this will be critical to the successful interoperability of OMG and Web technologies.