A Protection Scheme for Java Mobile Code

D. Hagimont

Project Sirac
Unité de Recherche INRIA Rhône-Alpes
655 avenue de l'Europe
38330 Montbonnot Saint-Martin - France
E-mail: Daniel.Hagimont@inrialpes.fr

Protection is a crucial aspect of distributed computing, in particular when users co-operate using shared resources. The development of distributed applications over the Internet has enhanced the interest for protection mechanisms: the Internet connection should not be a trap-door for the local host.

Sun Microsystems has recently made available an environment called Java, which allows the development of distributed applications through a C++ like language. The main innovation of Java is that it allows the management of mobile code. The code generated by the Java compiler is interpreted by the Java virtual machine, thus enabling code transfer between heterogeneous sites. In particular, several Web browsers that encapsulate a Java interpreter have been developed and are used for loading simple applications called applets which are pointed to by HTML pages.

More generally, mobile code is a means to structure distributed applications in terms of mobile agents. A mobile agent is a program with an execution context, which may migrate from one node to another according to its needs, using information and services provided by information servers available on the Internet.

In this context, it is crucial to allow servers to implement a protection policy that prevents untrusted agents from damaging the servers, without forbidding access to servers' resources. This protection scheme must allow access rights to evolve dynamically according to the execution context of the agent: an agent that invokes an object from a server may in return be granted access to other objects from the server.

In this regard, we have designed a capability-based protection scheme that we have integrated in the Java environment. This protection scheme manages untrusted mobile code in isolated protection domains. A protection domain is associated with a set of capabilities which determines the access rights in that domain. Capabilities may be exchanged between protection domains. An important feature of this protection scheme is that capability management is defined separately from the application code, by the application administrator.

Our current work consists in experimenting with this protection mechanisms for safely managing servers for mobile agents. An agent that executes on a server is initially given predefined capabilities in its protection domain, but it can be granted additional capabilities during its runtime on that server. These capabilities are hidden to the agent's programmer. The protection policy between an agent and the server, and between different agents, is specified by the server.