Journal of Automata, Languages and Combinatorics **11** (2006) 1, 59–106

A CONFINEMENT CRITERION FOR SECURELY EXECUTING MOBILE CODE [1]

HERVÉ GRALL[2]
École des mines de Nantes
La Chantrerie, 4, rue Alfred Kastler, B.P. 20722, 44307 Nantes Cedex 3, France
e-mail: hgrall@emn.fr

ABSTRACT

Mobile programs, like applets, are not only ubiquitous but also potentially malicious. We study the case where mobile programs are executed by a host system in a secured environment, in order to control the accesses from mobile programs to local resources. The article deals with the following question: how can we ensure that the local environment is secure? We answer by giving a *confinement criterion*: if the type of the local environment satisfies it, then no mobile program can directly access a local resource. The criterion, which is type-based and hence decidable, is valid for a functional language with references. By proving its validity, we solve a conjecture stated by Leroy and Rouaix at POPL '98. Moreover, we show that the criterion cannot be weakened by giving counter-examples for all the environment types that do not satisfy the criterion, and that it is pertinent by detailing the example of a specific security architecture. The main contribution of the article is the proof method, based on a language annotation that keeps track of code origin and that enables the study of the interaction frontier between the local code and the mobile code. The generalization of the method is finally discussed.

Keywords: Typed programming languages, mobile code, language-based security, access controls, confinement

1. Introduction

Mobile programs, like applets, are not only ubiquitous but also potentially malicious. It is thus usual that a host system executes mobile programs in a secured local environment. The environment acts as an interface for local resources and thus enables the control of the interactions between mobile programs and local resources, and particularly the accesses from mobile programs to local resources. A typical example is provided by the language Java, which was designed to support the construction of applications that import and execute untrusted code from across a network, like Internet. A Java applet, which is a mobile program, is executed in a secured environment by a virtual machine, which can be embedded in a web browser, or in a

[1] Full version of a submission presented at the *International Workshop on Security Analysis of Systems: Formalisms and Tools*, SASYFT 2004, (Orléans, France, June 21 – 22, 2004).

[2] This work was undertaken at CERMICS (ENPC – INRIA), école nationale des ponts et chaussées, France.