Proposal for Doctoral Dissertation - MAPi 2007

January 21, 2008

Topic

Mobile code security based on Kleene algebras and temporal logics

Supervisors

- Nelma Moreira (nam@ncc.up.pt), Departamento de Ciência de Computadores da FCUP
- Simão Sousa (desousa@di.ubi.pt), Departamento de Informática, Universidade da Beira Interior .

Research Unit

LIACC - Laboratório de Inteligência Artificial e Ciência de Computadores

Abstract

This work aims in contribute to the development of logic-based (source level) proof-carrying code systems. Proof-carrying code (PCC) aims in providing static security enforcement mechanisms based on the notion of safety certificate. Every PCC architecture define a balance between the expressiveness of the safety and security requirements, and the complexity of its formal

enforcement. Temporal logics have been successfully applied to hardware verification and more recently to formal verification of software, mainly in the context of model checking. Kleene algebras with tests subsume propositional Hoare logics and have been used for program static analysis. Both approaches have decidable decision problems and we plan to investigate their feasibility to the automatic production of certificates (instead of relying in a proof assistant) in the context of PCC.

Goals

One of the challenges of using formal methods for ensuring security policies in mobile code is their integration in the standard process of software development. It should be easy to guarantee several safety and security requirements in a transparent manner for the software engineer. All PCC architectures establish a compromise between the degree of security and the feasibility of its enforcement. Our proposal focus in studying and implement new ways of redefine this compromise. The main approach will be to identify and to tackle security and safety conditions that can be automatically generated.

In the context of logic-based formal software verification this proposal aims to

- allow a better automatic enforcement of security policies in mobile code
- explore the possible advantages of use Kleene algebras and temporal logics in the production of certificates in the context of PCC
- implement a platform for mobile code verification based on the results obtained in the previous items.

This work is part of the RESCUE Project (FCT/PTDC/EIA/65862/2006) which aims at providing innovative, efficient and expressive mechanisms for the secure implementation and execution of code, with an emphasis on problems posed by embedded systems.