Project number acronym: **IST-1999-29075 SecSafe**
Project title: **Secure and Safe Systems based on Static Analysis**
Key Action/Action line: **FET–Open**

Project Abstract

Static analysis of programs is a proven technology in the implementation of compilers and interpreters. Recent years have begun to see application of static analysis techniques in novel areas such as software validation and software re-engineering. This project will demonstrate that static analysis technology facilitates the validation of systems based on the internet and on smart cards.

Objectives

The objective of the project is to assess the scalability of static analysis technology to the validation of security and safety aspects of realistic languages and applications. We have identified two domains where security is all-important: smart cards and internet programming. We intend to develop methods that apply to both domains by focussing a substantial part of our efforts on the Java programming language and its dialect Java Card, treating source-level as well as bytecode-level applications.

Description of work

The project has 4 main tasks:

1. Specification of Security Properties: The objective of this task is to determine the most appropriate way of expressing the dynamic properties of interest for security and safety. We have some experience of using a linear-time temporal logic over program traces for expressing a variety of security properties. This task is an investigation of the scalability and extension of these techniques to realistic case studies.

2. Static Analysis: The focal point of the project is the development of analyses that, on the one hand, provide useful information for the security and safety of systems and, on the other hand, are able to deal with large programs that are subsequently modified. A number of promising approaches exist for developing suitable analyses with varying degrees of precision and cost: e.g. Type and Effect Systems and Flow Logics. Aspects of analysis techniques which are important are modularity and expressibility of control flow analysis.

3. Algorithms and Tools: The implementation of static analyses eventually boils down to constraint solving. We will aim at adapting general tools which are already available rather than performing ad hoc developments of new tools. As we extend analysis techniques to cope with larger languages, we may also need to extend the state-of-the-art in constraint solving.

4. Semantics: This task has two sub-parts: modularising semantic specifications and correctness proofs; and semantic specification of security-specific aspects of Java and Java

Card. Key technical challenges involve developing good semantic accounts of visibility modifiers and shareable interfaces.

Milestones and expected results

There will be 3 milestones; the milestones are at the end of each year of the project. The main results of the project will be papers and prototype systems for the validation of the security and safety of systems based on the internet and on smart cards.

Partcipants

Imperial College	UK
University of Aarhus	Denmark
INRIA	France
Trusted Logic S.A.	France

Total cost(euros): 1,635,806
Community funding(euros): 1,102,000
Project start and duration: August 2000, 36 months

Coordinator

Prof Chris Hankin
Dept of Computing
Imperial College
180 Queen's Gate
London SW7 2BZ
UK
tel: +44 20 7594 8266
fax: +44 20 7581 8024
e-mail: clh@doc.ic.ac.uk