

Java Card Application Side Channel Protection

MSc Research Project

Date: November 2, 2007

Introduction

Java Card is the most popular technology for the development of smart card applications. It speeds up the development process by relieving the application programmer of low level issues. As a consequence application programmers may have a good background in Java development, but lack a thorough understanding of typical smart card security issues.

Side Channel attacks are a security threat with large impact on smart card security. These attacks can be passive (observation and analysis), or active (fault injection). Smart card programmers aware of these threats can make their code defensive by hiding sensitive information and introducing fault tolerance.

Scope

Riscure has developed a series of secure programming patterns to assist developers in realising defensive code. A disadvantage of these patterns is that they decrease code maintainability and their application is labour intensive. The research question is to what extent the application of these patterns can be automated. A related research question is to automate the evaluation of the security strength of code (or optionally in CAP file format) against side channel aspects.

Research aspects

The following aspects should be addressed by the research:

- Study of side channel attacks and typical threat model.
- Review of the proposed secure programming patterns.
- Development of a model for automated analysis and application of programming patterns.
- Design of software prototypes for automated analysis and automated application of programming patterns.
- Implementation and test of prototypes both for Java source code and CAP files.
- Write an article for a scientific conference or magazine.

Conditions

The research will be performed at Riscure in Delft. Riscure provides a monthly allowance and, if necessary, housing costs for the duration of the research. A Riscure security analyst will be available for guidance and support. The project will result in a publication and a prototype. Riscure may pose restrictions to the distribution of this material. Riscure maintains the intellectual property rights over the results.

Students with a strong background in Java and an interest in information security are invited to send their resume and a motivation to:

Amanda van den Berg
Office Manager
Email: vandenbergr@riscure.com
Phone: +31 152682664
Web: www.riscure.com