

Side Channel Protection in Smart Cards

MSc Research Project

Date: November 2, 2007

Introduction

Side Channel attacks are a security threat with large impact on smart card security. Side channel analysis involves observation of power consumption, timing and electro-magnetic radiation to retrieve secrets like cryptographic keys and PIN codes. Smart card programmers can make their code defensive by implementing countermeasures, e.g. to hide sensitive information.

Scope

Riscure is a security lab involved in testing side channel resistance of smart card implementations. For the improvement of analysis methods it is important to get a thorough understanding of the leakage models of the applied hardware and countermeasures. Therefore it is interesting to develop a reference smart card implementation running cryptographic algorithms with various configurable side channel protection levels.

Research aspects

The objective is to develop and test configurable cryptographic algorithms in a smart card that is programmable at machine code level. The following aspects should be addressed by the research:

- Study of side channel attacks and typical threat model.
- Review of various countermeasures applied in smart cards.
- Design countermeasures for available sample cards.
- Implement reference cryptographic algorithm(s) with configurable countermeasures.
- Development of an application protocol for selecting and running algorithms.
- Test and compare leakage and strength of implementations.
- 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 C and an interest in information security are invited to send their resume and a motivation to:

Amanda van den Berg

Office Manager

Email: vandenberg@riscure.com

Phone: +31152682664

Web: www.riscure.com