Summary

Kristian M. Thomsen and Christoffer Ndũrũ

May 31, 2016

1 Summary

In May 2011 the Economic Interest Group discovered that smart cards stolen in France were being used for transactions in Belgium. It turned out a group of criminals had managed to bypass the PIN verification on the cards and could use them for purchasing items, which they would later sell on the black market. Since smart cards are a widespread technology, for example in credit cards, abuse of them poses serious risks to both the banking industry, but also to consumers.

This report presents fault injections on the Java Card platform. It is based on previous work formalising a subset of Java Card bytecode and fault models. The architecture of the Java Card platform is presented and how persistent and transient faults can affect it.

An approach to automatic conversion of Java bytecode to UPPAAL models is also detailed. In extension, approaches for automatic modelling of a variety of fault injection attacks are described. Several known fault injection countermeasures are also presented, accompanied by a solution to automate model based safety analysis of Java Card programs, by inserting attacks into code modified with countermeasures, and modelling them in the modelling tool UPPAAL.

The solution uses the tool *Sawja* to provide a convenient representation of Java bytecode, which makes bytecode more readable. The tool is able to produce call graphs of programs, which can be used for automation of countermeasures. Improvements to the solution are also offered to allow future work, including suggestions for the first steps in automating implementation of control flow and control graph integrity countermeasures, which could be used to create a solution that can compare countermeasures' abilities to protect against fault injections.

A series of experiments are also conducted in an attempt to compare countermeasures' protection level against two selected code bases. In extension, we explore the viability of our experiment approach used to compare countermeasures.