Java card software analysis using model checking

(summary)

author: Hugo Brakman
supervisors: Erik Poll, Wojciech Mostowski and Frits Vaandrager
research number: 568

Smart cards are used for a number of purposes. They are fitted on bank cards, used in mobile phones and many other products. The cards often contain confidential or secret data. A high level of security is therefore required. However, smart cards are easily obtained by assailants and tampering with them can be as easy as removing the card from its external power supply half way computation. The implementation of the software operating on the card can sometimes provide security against attacks on the hardware.

We consider Java cards, smart cards that allow for the execution of Java applications.
In this thesis we investigate the use of model checking in combination with fault injection in verifying the robustness of software on the Java card against different attacks on its hardware. We implemented an experimental tool that automatically generates a model from Java code, allowing for attacks to occur. We used this tool to generate models to verify the security of our running example, a PIN implementation, against different attacks. This supports our idea that automatic generation of such models directly from code can help developers to speed up the process of creating robust implementations that can withstand hardware attacks.