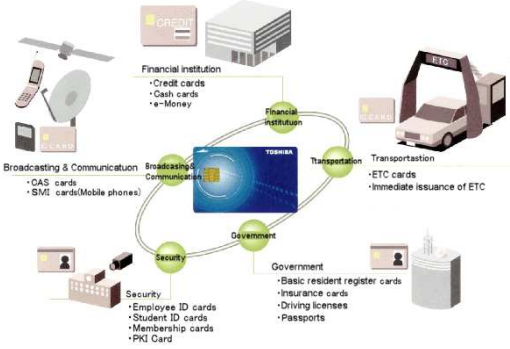
PINPAS Java Card

Program Inferred Power-Analysis in Software for Java Card

PINPAS JC

Background

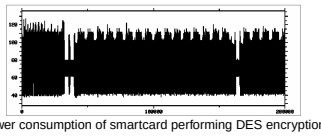
Smartcards are tamper-resistant miniature computers carrying secret material. They play a vital role in ICT security, eg. as bank cards, cash cards, GSM SIM cards, and the new biometric passport.



Smartcards are not 100% secure: there is an ongoing arms race in which new attacks on smartcards and countermeasures alternate. Therefore smartcards are subjected to rigorous **security evaluations** by independent evaluators.

Trends

- The main threat to smartcards today are **side-channel attacks** on underlying hardware:
  - passive side-channel attacks, which attempt to retrieve secret cryptographic keys by monitoring physical characteristics eg. timing, power consumption (SPA/DPA), EM radiation, ...



Power consumption of smartcard performing DES encryption

  - active side-channel attacks or fault injections, where cards are manipulated to induce faults, to by-pass security mechanisms or retrieve keys, eg. manipulating power supply or clock pulse, subjecting chip surface to heat or light (eg. using lasers), or EM radiation, ...
- Smartcard software is increasingly often written in the high-level programming language **Java**

Research Questions and Goals

Can we *predict* and *prevent* vulnerabilities of Java Cards to passive and active side-channel attacks?

Planned steps in answering these questions:

- a **software simulator** to easily observe vulnerabilities before software is implemented on a smartcard;
- **coding guidelines** to avoid vulnerabilities;
- **program analysis tools** to help detecting vulnerabilities.

Initial results:

- The PINPAS tool, a software simulator for side-channel analysis developed within the project, currently handles **SPA** and **DPA**, and provides **multiple key-management**.
- A simple yet effective **operation-based metric** has been proposed for the vulnerability evaluations of instructions to DPA attacks.
- Compliance to **JavaCard 2.1.1** upto **2.2.1** and **Global Platform** has been assessed for a number of commercially available JavaCards. Deviation from the standards may lead to vulnerabilities.
- Successfull verification of security properties w.r.t. **faults** caused by **card tears** has been conducted based on a case-study of counting failed PIN tries. The specification languages involved are **JML** and **temporal logic** with verification support from **model checkers** and the KeY tool. Some promising first steps have been taken towards formal verification of the JavaCard **transaction mechanism** using and KeY.

More info

Project webpage **www.win.tue.nl/pinpasjc/**

PINPAS JC is financially supported by SENTINELS a security research programme funded by

- Technology Foundation STW
- NWO
- Dutch Ministry of Economic Affairs

TU/e Technische Universiteit Eindhoven University of Technology

Radboud Universiteit Nijmegen

brightsight your partner in security approval