



PINPAS Java Card



Program Inferred Power-Analysis in Software for Java Card

Background

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

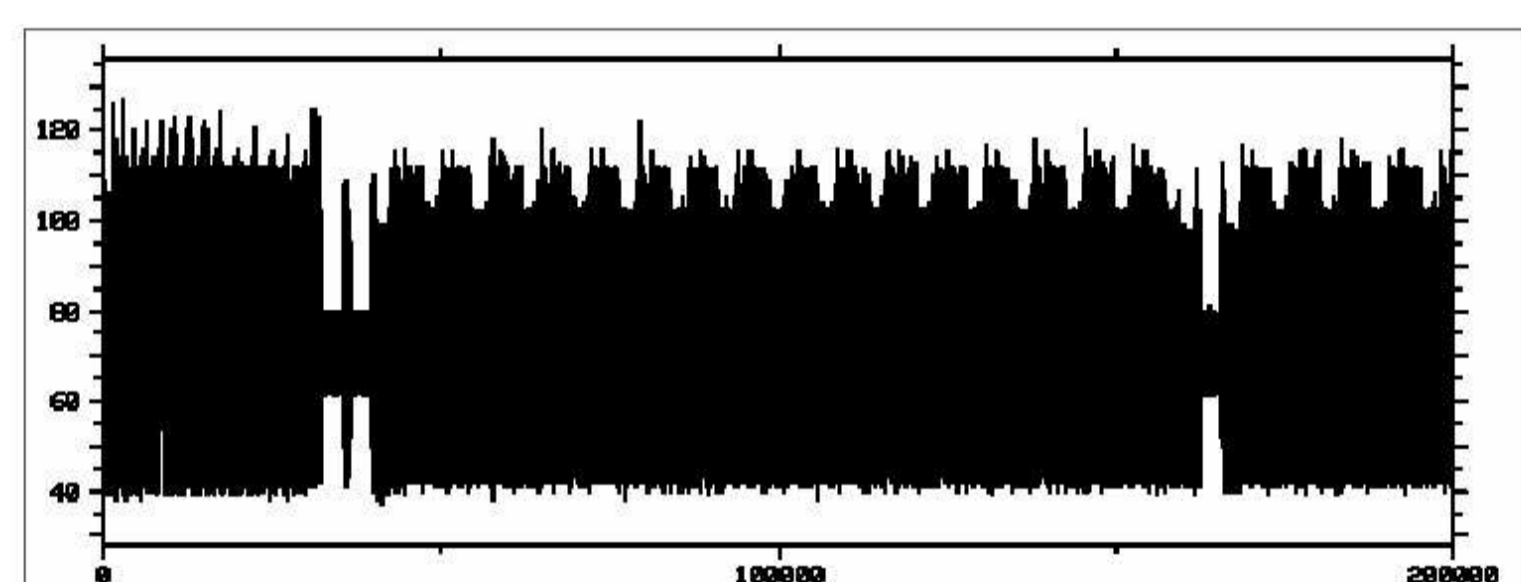
Smartcards are not 100% sure: there is an ongoing arms race in which new attacks on smartcards and countermeasures alternate. Therefore smartcards are subjected to rigorous **security evaluations** by independent evaluators such as TNO-ITSEF.

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 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 put on the physical smartcard;
- **coding guidelines** to avoid vulnerabilities;
- **program analysis tools** to help in detecting vulnerabilities.

Starting points for this work:

- the PINPAS tool by TU/e, a software simulator for passive side-channel analysis on low-level machine code programs;
- work on functional verification of Java Card programs at RU.

Partners

Research conducted at

- **Eindhoven University of Technology (TU/e)**
- **Radboud University Nijmegen (RU)**
- **TNO IT Security Evaluation Facility (TNO-ITSEF)**
- **University of Twente (UT)**

with case-studies provided by

- **STMicroelectronics, Belgium** 
- **Giesecke&Devrient, Germany** 

More info

- Erik de Vink (project leader, TU/e) evink@win.tue.nl
- Jerry den Hartog (UT) j.i.denhartog@cs.utwente.nl
- Erik Poll (RU) erikpoll@cs.ru.nl
- Jaap de Vos (TNO-ITSEF) vos@itsef.com

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

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



Radboud Universiteit Nijmegen

