~~Fault Analysis Study of IDEA~~

Physical Security of Embedded Cryptographic Devices

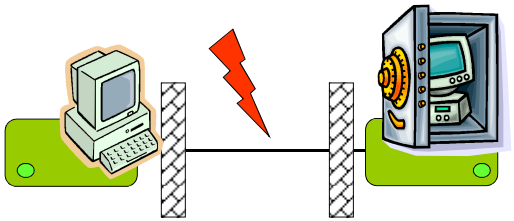
Benedikt Gierlichs
benedikt.gierlichs@esat.kuleuven.be

K.U.Leuven, ESAT- SCD - COSIC
Computer Security and Industrial Cryptography
www.cosic.be

Embedded Cryptographic Devices

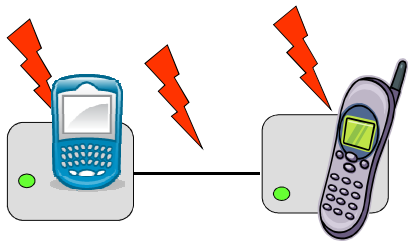
- A cryptographic device is an electronic device that implements a cryptographic algorithm and stores a cryptographic key. It is capable of performing cryptographic operations using that key.
- Embedded: it is exposed to adversaries in a hostile environment; full physical access, no time constraints

Security



Old Model (simplified view):
-Attack on channel ***between*** communicating parties
-Cryptographic operations in ***black*** boxes
-Protect link with strong cryptography
-Provable, computational, etc. security

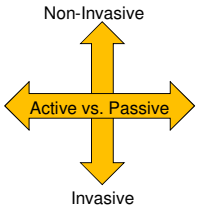
Embedded Security



New Model (also simplified view):
-Attack on channel ***and*** endpoints
-Cryptographic operations in ***gray*** boxes
-Protect link with strong cryptography
-Protect cryptography by secure implementation

Classifications of Physical Attacks

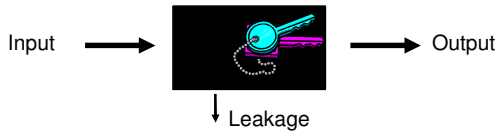
- Active versus passive
  - Active: Perturbate and conclude
  - Passive: Observe and infer
- Invasive versus non-invasive
  - Invasive: bus probing
  - Non-invasive: observe timing behaviour



- Side channel: passive and non-invasive
  - Very difficult to detect
  - Often cheap to set-up
  - Often: need lots of measurements
- Circuit modification: active and invasive
  - Expensive to detect invasion
  - Very expensive equipment and expertise required

Side-Channel Leakage

- Physical attacks ≠ Cryptanalysis
  (gray box, physics) (black box, maths)
- Does not tackle the algorithm's math. security



- Timing, Power, EM, Light, Sound, Temperature
- Observe physical quantities in the device's vincinity and use additional information during cryptanalysis

Principle is nothing new...

"Breaking into a Safe is hard, because one has to solve a single, very hard problem..."

"Things are different if it is possible to solve many small problems instead..."

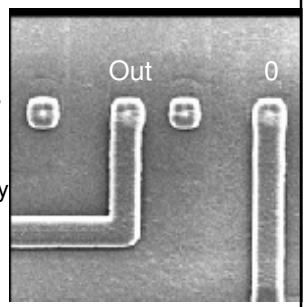
"Divide et impera!"

Provable Physical Security?

- Relatively new field of research
- Initiated by Mikali & Reyzin
- Attempt to prove security of an abstract computer with a leakage function
  - Very generic model, strongest possible adversary
  - Hard to work with in Practice
  - Considers 'only' passive adversaries
- Standaert et al. attempt to restrict model and adversary to realistic cases
  - Model is more useful, still only passive...

Active Attacks

- Invasive: modify circuits (worst nightmare...)
  - Cut or Paste tracks with laser or focused ion beam: insecurity à la carte
  - Disconnect security mechanism
    - Deactivate security sensors
    - RNG stuck at a fixed value
    - Reconstruct blown fuses
  - Add probing pads on buried lay



[www.fa-mal.com]

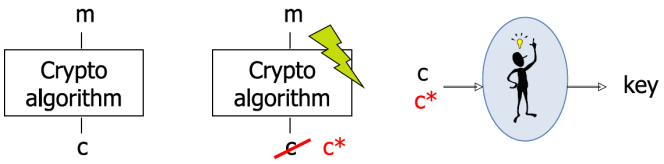
Active Attacks

- Semi-Invasive: exploit faulty behavior provoked by physical stress applied to the device
  - Laser fault injection allows to target a relatively small surface area of the target device
  - Laser pulse frequency ~ 50Hz
  - Fully automated scan of chip surface
  - Once you have a weak spot: perturbate and exploit

[www.new-wave.com]

Differential Fault Analysis

- Ask for a cryptographic computation twice
  - With any input and no fault (reference)
  - With the same input and fault injection
- Infer information about the key from the output differential



- Allows to work in the Random fault model

Provable Physical Security facing all this?

- If you have a bit of spare time, why not...
  - Include active adversaries in the models of Micali and Reyzin, Standaert et al.
  - Try to give a reasonable formal definition of an active adversary (some first steps are done here)
  - (Dis-)Prove that a certain level of security can be guaranteed

Thank you. Questions?

Lesson to be learned:

Implementation of security

≠

Secure implementation

... and if you are interested in the talk
„Fault Analysis Study of IDEA“...
http://homes.esat.kuleuven.be/~bgierlic