Electro-Magnetic Fault Injection

Research Project
Universiteit van Amsterdam
SNE OS3

Sebastian Carlier
(sebastian.carlier@os3.nl)

February 8, 2012

Introduction

Approach

Tests

Conclusion

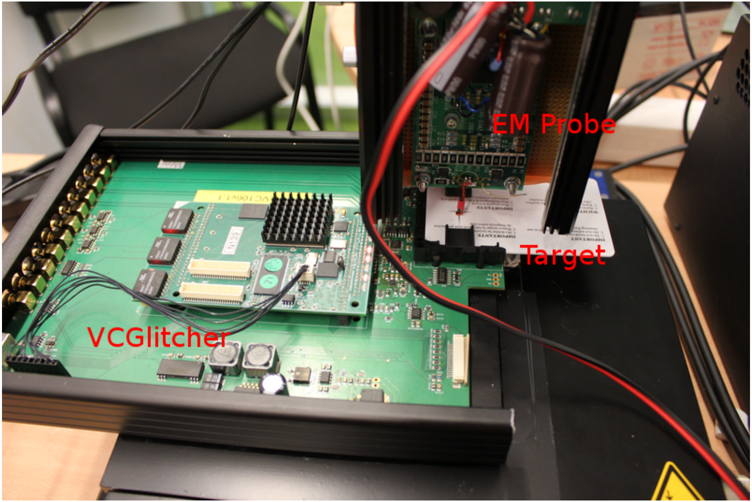
Demo

Research Question

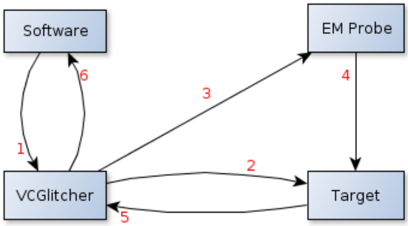
Is EMFI feasible on embedded systems / smartcards?

- *What is the most efficient configuration of the used EM probe?*

Setup

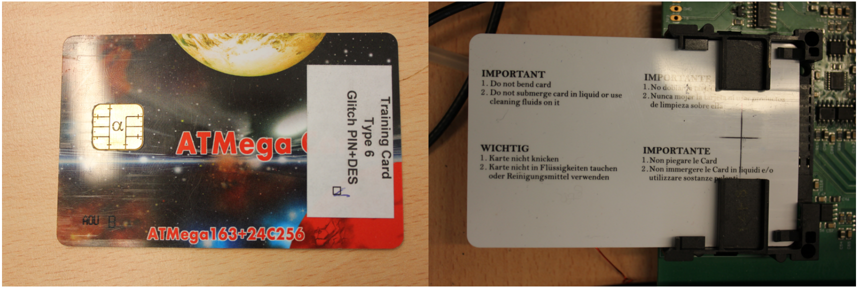


How it works

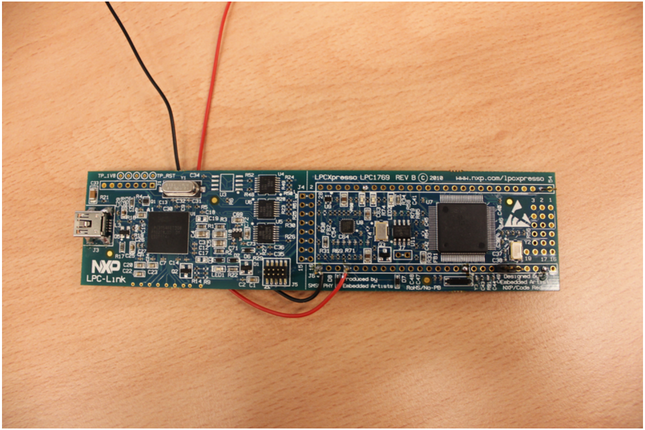


1. send software parameters
2. start target
3. start probe with software parameters
4. perform glitching
5. return output
6. return output from target

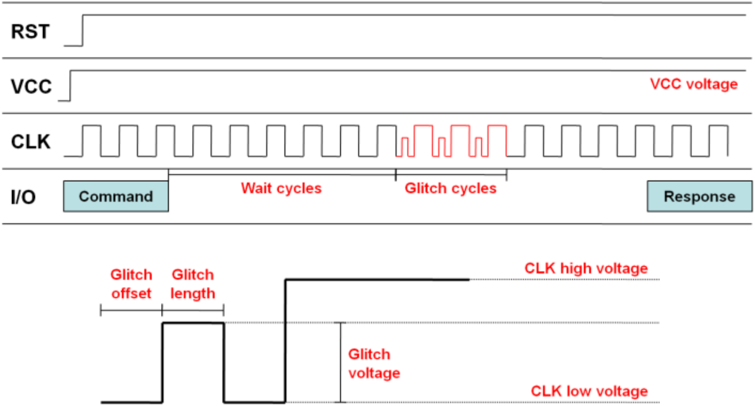
Smartcard - ATMega163


ATMega
ATMega163+24C256
Training Card
Type 6
Glitch PIN+DES
IMPORTANT
1. Do not bend card
2. Do not submerge card in liquid or use cleaning fluids on it
WICHTIG
1. Karte nicht knicken
2. Karte nicht in Flüssigkeiten tauchen oder Reinigungsmittel verwenden
IMPORTANTE
de limpieza sobre ella
IMPORTANTE
1. Non piegare le Card
2. Non immergere le Card in liquidi e/o utilizzare sostanze

Embedded chip - LPCExpresso1769



Target specific parameters



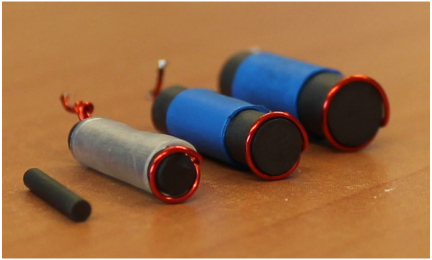
...and coil position over the chip.

Source: Inspector 4.4 User's Manual.

Target independent parameters

Target independent:

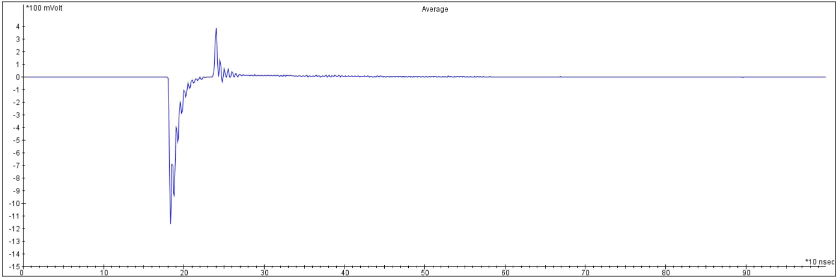
- coil diameter/shape
- distance
- EM probe voltage



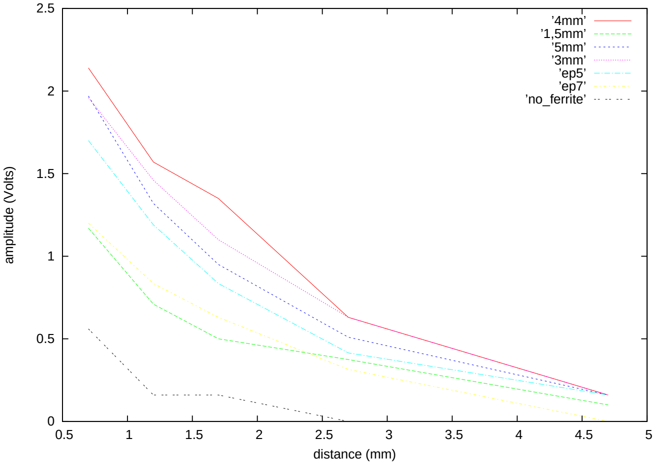
Approach

1. test target specific parameters randomly
2. save fault inducing parameters
3. test target independent parameters:
   - measure the effect of each parameter
   - compare the success rates

the glitch


*100 mVolt
Average
4
3
2
1
0
-1
-2
-3
-4
-5
-6
-7
-8
-9
-10
-11
-12
-13
-14
-15
0
10
20
30
40
50
60
70
80
90
*10 nsec

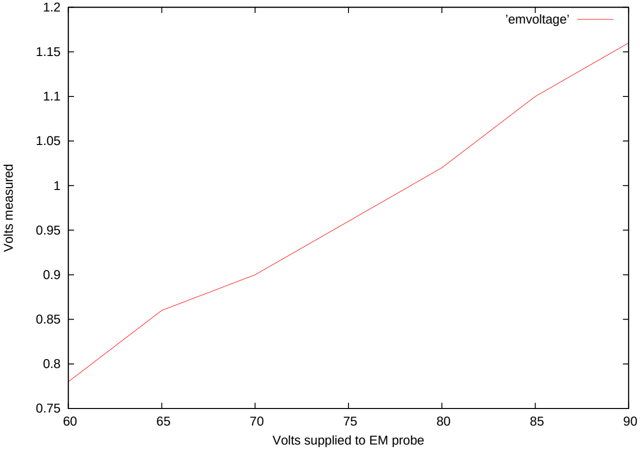
coil and distance



EM Probe Voltage

- 1.5mm coil
- minimum distance - 0.7mm
- tested from 60V to 90V in 5V increments

EM Probe Voltage



Tests

Other interesting results (1000 iterations on smartcard):

- 1,5mm coil:
    - 80V: 0 timed out, 0 glitched
    - 85V: 0 timed out, 9% glitched
    - 90V: 0 timed out, 20% glitched
- 4mm coil:
    - 80V: 13% timed out, 19% glitched
    - 85V: 15% timed out, 21% glitched
    - 90V: 23% timed out, 23% glitched

Tests

Other interesting results (1000 iterations on embedded chip):

- 1,5mm coil, 90V: 0% glitched
- 4mm coil:
  - 85V: 0% glitched
  - 87,5V: 3% glitched
  - 90V: 0% timed out, 8% glitched

Conclusion

Is EMFI feasible on embedded systems and smartcards?
Yes.
The parameters:

- Distance is the most relevant.
- Type of the coil can heavily influence the success rate as well as time outs.
- EM Probe Voltage has a lesser effect.

Future Research

Supply the probe with more voltage to:

- test more resistant targets
- achieve a higher success ratio

Demo

Questions?