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

- **VCGLitcher**
- **Target**
- **EM Probe**
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
Embedded chip - LPCExpresso1769
Target specific parameters

...and coil position over the chip.

Target independent parameters

- coil diameter/shape
- distance
- EM probe voltage
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
coil and distance

![Graph showing the relationship between amplitude (Volts) and distance (mm) for different coils and distances.](graph.png)
EM Probe Voltage

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

The graph shows the relationship between volts supplied to the EM probe and volts measured. As the volts supplied increase from 60 to 90, the volts measured also increase linearly from approximately 0.75 to 1.2. The label 'emvoltage' is plotted on the graph.
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
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.
Supply the probe with more voltage to:

▸ test more resistant targets
▸ achieve a higher success ratio
Demo
Questions?