

# Course Syllabus

|  |
| --- |
| **Block 1. Tools and attacks** |
| We start with an overview of the state-of-the-art choices available to perform FI attacks. Next, you design and build a setup which can carry out a complex FI attack and use tools that allow decisions to be made in real-time. Further, we show how data mining tools can help increase the success rate of your experiments by using real time information to reduce the parameters search space. |

Block 1. State of the art: Tools and Attacks

* Body Biasing injection (BBI) -precision localized

glitches with high power electrical pulses

* Dual laser attacks with twin scan technology
* Biasing true random number generators with EM

harmonic emission

* Perform double glitches and/or combine multiple trigger sources
* Create real-time scripts which allow nano-second precision control of the setup
* Visualize experiment results using data mining

tooling an introduction

Block 2. Implementing complex leakage models

* Use data post-processing to gain more insight

into FI results.

* Reduce the complexity of an FI attackby breaking down the testing into falsifiable/simple tests.

|  |
| --- |
| **Block 2. Deep Analysis** |
| The main learning goal is to understand experiment results and know how to perform a sanity check of your setup and the  results. We use visualization, post-processing and filtering  of the results to reduce the parameter search space.  For this session we use modern targets representative for a market segment, e.g. automotive, or with typical countermeasures. Analysis is performed on collected data sets. |

* Use backside imagining/floorplans and FI results

to navigate the die.

# Case study: secure boot

* Identify sensitive points in the secure boot

process

* Prerequisites for attacking each sensitive point
* Break down the attack(s) into simple falsifiable tests

# Case study: Characterization ofa SoC

* Simple tests to identify fault models
* Hardware elements susceptible to faults: where did the fault occur?
* Software constructs susceptible to faults
* Knowing the fault models: how can your

implementation be improved?

Block 3. FI in the dark

|  |
| --- |
| **Block 3. FI in the Dark** |
| Direct messages from your target are not the only source of information. A side channel can provide insight into the behavior of the target. The learning objective is to identify additional sources of information and use them. |

* Identify side channels applicable for a test

scenario to gather information

* Combine side channels and existing results to

increase the attacksuccess rates.

Case study: DFA-protected AES implementation

Case study: target without serial output.