

**Course Syllabus**

CPA recap

* Brief intro to SCA: tools, acquisition and

process overview

* Walk & Explore: acquisition, alignment

|  |
| --- |
| Day 1. Template analysis and beyond |
| We kickstart the training with a side channel analysis refresher, a brief but thorough recap of the most common terms and practices, including the basics of signal acquisition, processing and modelling of data dependencies.  We move on to leakage detection and thus introduce the *t*- test and the Test Vector Leakage Assessment (TVLA) methodology. We show how to apply this methodology in order to select the hotspot for a set of EM measurements, and subsequently discuss the strengths and limitations of such an approach.  We next discuss template attacks, the strongest attacks from an information-theoretic perspective. We  discuss in detail topics such as points of interest (POI) selection, profiling and attack efficiency. Subsequently, we discuss the use of custom leakage models and show how to create them. |

* Power analysis: correlation power analysis (CPA)
* Signal processing

𝑡-test for hotspot finding and TVLA

* Limitations of basic EM hotspot search
* 𝑡-test for finding the EM hotspot
* TVLA for leakage detection

Template analysis

* Theory of template analysis
* Points of Interest (POI) selection
* Template attacks in practice
* SPA-like template attacks
* DPA-like template attacks

Implementing complex leakage models

* Leakage modeling in DPA
* Common leakage models (e.g. Hamming

weight, Single-bit, etc.)

* Weighted linear leakage model
* Create and use custom leakage models in Inspector

Chosen plaintext attacks on AES:

|  |
| --- |
| Day 2. SCA on advanced/protected crypto |
| We apply the knowledge from the first day to attack a modern AES implementation using a chosen plaintext attack and elliptic curve signatures. We perform higher-order analysis on 𝑚-ary RSA implementation. Due to popular demand, we have a special session dedicated to communication protocols with proprietary targets using a proxy (we use python). All concepts are illustrated with practical exercises which are designed to consolidate your understanding. |

* AES reference design
* Efficient implementations of AES in Software

and Hardware

* Perform a chosen plaintext attack on optimized AES

Attacks on byte-multiply (ECC, ECDSA, DSA)

* ECC byte-multiply attacks
* Acquiring traces in the presence of high jitter
* Key retrieval from an ECNR implementation

Second order DPA on masked AES

* Masking AES implementations
* Second order attacks to bypass masking

Higher-order RSA 𝑚-ary exponentiation

* RSA implementation in OpenSSL
* Message blinding
* Cross-correlation attacks

Create a proxy for Inspector (Communication with proprietary targets)