Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis, Master's Thesis

Deep Learning Techniques for Side-Channel Attack

In side-channel analysis (SCA), an attacker exploits information leakage from power measurements, EM emanations and other sources to obtain the secret of the target device. PowerfulSCA attacks such as Template Attacks struggle under suboptimal conditions such as desyncronized traces and clock jitter in the DUT.

Recently, Deep Learning techniques have been proposed [1,2] to improve SCA. Furthermore, different data sets have been published [1,3] enabling the evaluation and comparison of different Deep Learning algorithms.

Depending on your background and type of work, possible tasks of this project include

- Develop a Convolutional Neural Network for SCA on existing datasets
- Compare Deep Learning Techniques to classical SCA (CPA, Template Attacks, ...)
- Create further datasets as base for machine learning evaluations.

This work can be conducted in English or German. In case of high quality of the work, results might be published.

References

[1] Prouff et al.: Study of Deep Learning Techniques for Side-Channel Analysis and Intro-duction to ASCAD Database, Cryptology ePrint Archive, Report 2018/053
[2] Cagli et al.: Convolutional Neural Networks with Data Augmentation Against Jitter-BasedCountermeasures, CHES 2017
[3] Riscure CHES 2018 CTF: https://chesctf.riscure.com/2018/content?show=training

Prerequisites

- Basic understanding of machine learning algorithms (e.g. Neural Networks, ...)
- Basic understanding of side-channel analysis (e.g. from visiting the lecture Sichere Implementierung kryptographischer Algorithmen and/or Smart Card Lab)
- Good programming skills in Python, ideally experience with Tensorflow and/or Pytorch

Contact

Technische Universität München
Lehrstuhl für Sicherheit in der Informationstechnik
Lars Tebelmann / Thomas Schamberger
Theresientr. 90, N1010
E-Mail: lars.tebelmann@tum.de / thomas.schamberger@tum.de

Advisors

Lars Tebelmann, Thomas Schamberger