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

Master's Thesis

Utilizing Machine Learning in Side Channel Analysis (AISEC)

In the Side Channel Analysis community Machine Learning (ML) is mainly used in exchange to classic statistics on algorithmic level. Yet, the supremacy of this approach has not been shown. The effort to find a point of interest and the creation of working ML models often exceeds the effort of classic approaches.
Another approach focuses on the hardware instead of the algorithm. This thesis has a two-fold goal. In a first step the thesis should clarify if ML can be utilized to infer instructions executed on a microcontroller. Some results have been shown by [1] and [2] without the use of advanced ML algorithms.
Second the extracted model should be evaluated with respect to an enhanced search for points of interest in cryptographic algorithms.

Prerequisites

- Basic knowledge of statistics.
- Previous experience in the field of Side Channel Attacks.
- Very good programming skills (Python, C).
- (Optional) Machine-Learning experience.
- Optional) Experience with assembly.

Contact

Emanuele Strieder
Telefon: +49 89 322-9986-140
E-Mail: emanuele.strieder@aisec.fraunhofer.de

Marc Schink
Telefon: +49 89 322-9986-144
E-Mail: marc.schink@aisec.fraunhofer.de

Fraunhofer Research Institution for Applied and Integrated Security (AISEC)
Department Hardware Security
Parkring 4, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de
Date of publication: 13. Februar 2020

Advisors

Georg Sigl
Emanuele Strieder + Marc Schink (Fraunhofer AISEC)