Project 1: Robust Deep-learning-based Side-Channel Attacks

Channing Smith
College of Charleston

Joel Ward
Cedarville University

Dr. Boyang Wang
University of Cincinnati

Chenggang Wang
University of Cincinnati

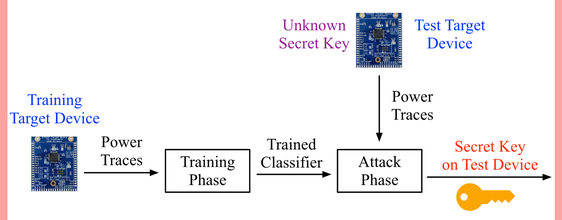
Dr. Marty Emmert
University of Cincinnati

Abstract

We study the effects of different variables on a new SCA method called TripletPower, a model that utilizes a triplet network and is more robust in the cross-device scenario. We collect multiple EM datasets from XMEGA and STM32F3 microcontrollers in order to see if the method is able to recover keys correctly after training and testing. We also study the effects of instruction rewriting on the model.

Background

Side channel attacks aim to recover sensitive information about a process by analyzing information that a system inadvertently leaks.



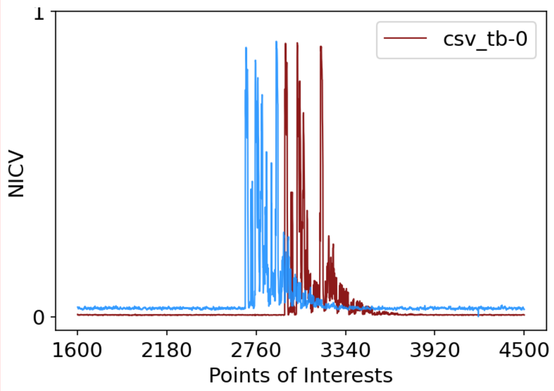
Objectives

- Study instruction rewriting in assembly on AVR XMEGA and Arm STM32 as well as examine the impact of instructions rewriting in deeplearning cross-device side channel attacks
- Collect EM and power traces on microcontrollers and test results with our existing ML code

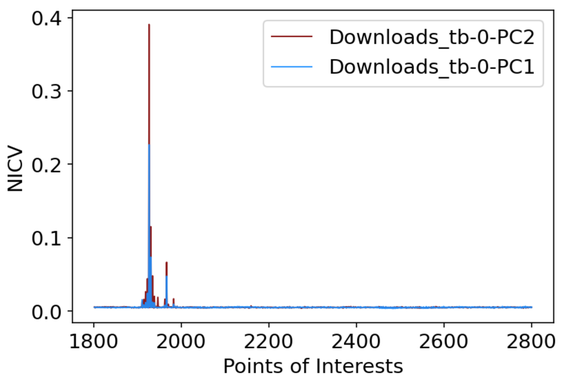
Methods

Collecting EM Traces/Instruction Rewriting

- Rewrite instructions in assembly
- Decide on a key, collect, and split dataset of 50k traces
- Test NICV & CPA
- Train/Test CNN with 40k traces and 10k traces



Masked vs. rewritten masked AES NICV results



PC1 vs. PC2 unmasked XMEGA NICV results

Results

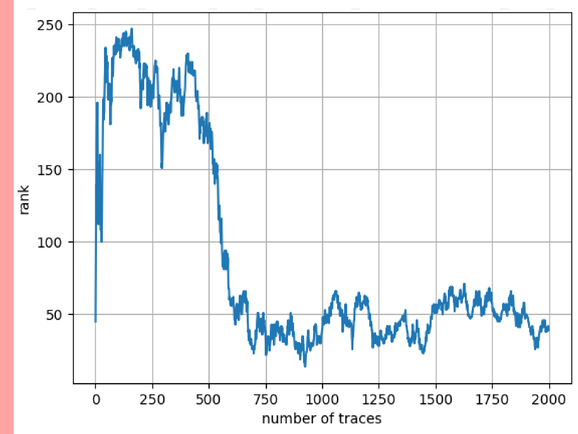
Collecting EM Traces

- CNN trained on 40k unmasked AES EM traces failed to recover the key with 10k EM traces from cross-device setting.
- CNN trained on 40k masked AES EM traces failed to recover the key with 10k EM traces from cross-device setting.
- NICV and CPA completed on STM32, but was very noisy.

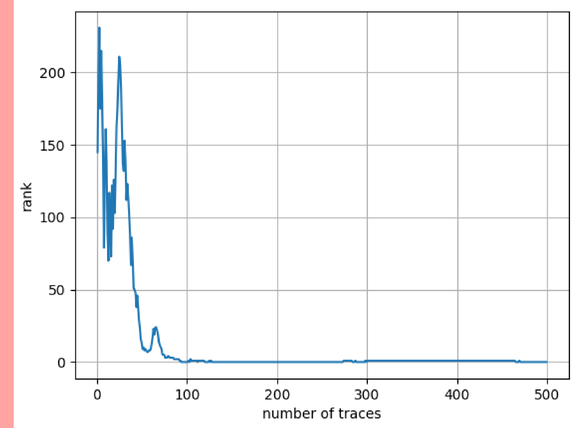
Set up of the datat collection from XMEGA board using EM probe.

Instruction Rewriting

- CNN trained on 40k masked AES power traces failed to recover key with 10k rewritten power traces and attack window of [1600,4500]
- CNN trained on 40k masked AES power traces recovered key with 10k rewritten power traces and adjusted attack window of [1900,4800]. Key rank converged to 0 within 200 traces
- CNN trained on 40k rewritten AES power traces recovered key with 10k rewritten power traces and attack window of [1600,4500]. Key rank converged to 0 within 35 trace



Key rank of rewritten AES traces tested on CNN trained with masked AES traces with attack window of [1600,4500]



Key rank of rewritten AES traces tested on CNN trained with masked AES traces with attack window of [1900,4800]

Acknowledgments

This work is supported by National Science Foundation (NSF), CNS-2150086, RHEST: NSF REU Site In Hardware and Embedded Systems Security and Trust