Review of AISY Research Paper

E/17/038 Anuruddha

E/17/101 Anjalee

E/17/292 Rilwan

Overview

- a deep learning-based framework for profiling side-channel analysis
- enables the users to run the analyses and report the results efficiently
- Maintain results’ reproducible nature
- Use supervised machine learning - multi class classification
- Use deep neural network with softmax output layer

Advantages

- Maintain results’ reproducible nature
- Easy to use - built on top of Keras library
- Integrated Database
- Provide a web application
- One-click Script Generation
- State-of-the-art side-channel analysis
- Team work

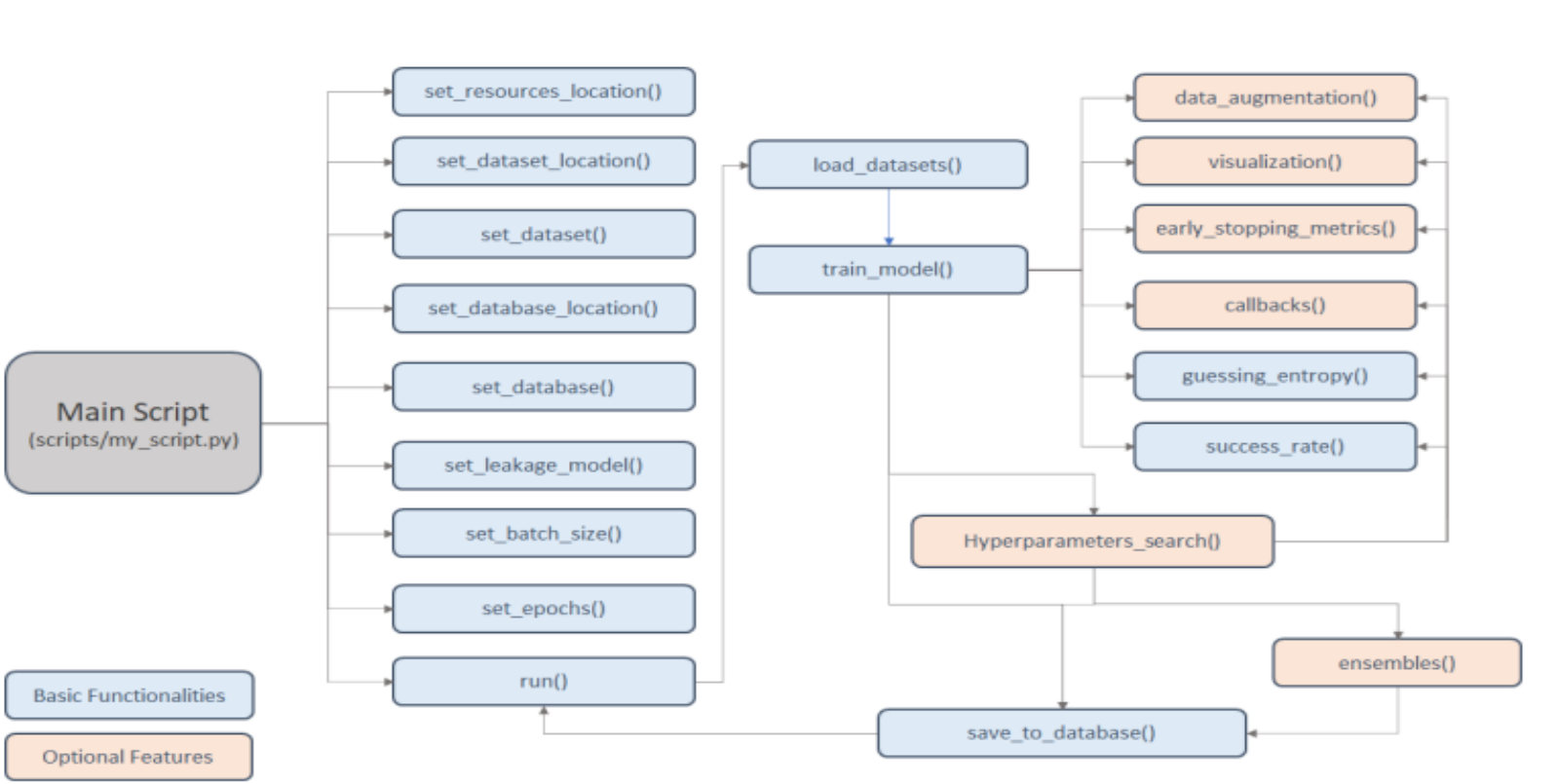
Profiling and Attacking

- In SCA, the profiling phase is the same as the training in ML
- In the attack phase, the goal is to make predictions about the classes
- Aims to reveal the secret key k^*. For this partial guessing entropy is used in AISY framework

General Design

- Current framework version is 1.0
- Open-source
- Currently, the AISY framework supports deep learning-based SCA for the AES cipher with 128-bit key

Framework flow



Layout

```
custom/                                 # folder containing customized definitions
    custom_callbacks/callbacks.py       # file with user callbacks
    custom_metrics/                     # each .py file contain a custom metric
    custom_models/neural_networks.py    # file to insert user neural networks (keras models)
    custom_datasets/datasets.py         # file with dataset details
    custom_data_augmentation/           # file containing data augmentation method
    custom_tables/tables.py             # file containing custom sqlite tables
resources/                              # folder to store user resources (created when first analysis executed)
    databases/                          # .sqlite database files with project information and analysis results
    figures/                            # .png figure generated from user
    models/                             # .h5 models
    npz/                                # .npz files with project information and analysis results
scripts/                                # folder to store main user scripts
webapp/                                 # flask web application files (html, js, css)
app.py                                  # main flask application
```

Datasets

- Currently 5 datasets are supported in the framework
- only format currently supported is .h5, where datasets need to be generated according to the ASCAD database description

ASCAD Fixed Key

- target - an 8-bit AVR microcontroller running a masked AES-128 implementation, where the side-channel is electromagnetic emanation
- Profiling - 50 000 traces
- Testing - 10 000 traces
- Provides the preselected window of 700 samples to attack first masked byte

Datasets (Continued)

ASCAD Random Keys

- Target - same as ASCAD Fixed Key dataset
- Profiling - Has random keys, 200 000 traces
- Testing - a fixed key, 100 000 traces
- Provides the preselected window of 1 400 samples to attack first masked key byte

CHES CTF 2018

- Target - masked AES-128 encryption running on a 32-bit STM microcontroller
- Profiling - contains a fixed key, 45 000 traces
- Testing - fixed key different from the key configured for training and validation set, 5 000 traces
- Each trace consists of 2 200 samples

Datasets (Continued)

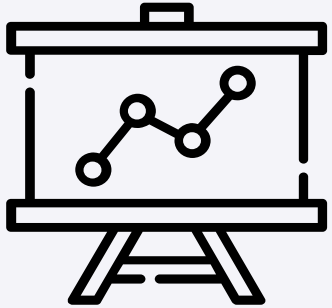
AES HD

- Target - unprotected hardware implementation of AES-128 implemented on Xilinx Virtex-5 FPGA of a SASEBO GII evaluation board
- Contains 50 000 traces
- Each trace has 1250 samples

AES HD ext

- AES HD extended dataset
- Contains 500 000 traces
- Each trace has 1250 samples

Standard Metrics



- Guessing Entropy

  To compute guessing entropy, a user must define the key rank calculation definition

- Success Rate

  Automatically computed together with guessing entropy

- Accuracy
- Loss

} estimated for each epoch during training

Neural Network Models

- Allows deep learning analysis with multilayer perceptron and convolution neural networks
- To allow easier usage of the AISY framework, authors also implemented several state-of-the-art architectures
    (1) ASCAD mlp
    (2) ASCAD cnn
    (3) methodology cnn ascad
    (4) methodology cnn aeshd
    (5) methodology cnn aesrd
    (6) methodology cnn dpav4 [43]

Leakage Models

- Supports 4 different leakage models
    - (01) Bit - results in 2 classes
    - (02) Hamming weight - results in 9 classes
    - (03) Hamming distance - results in 9 classes, need to consider 2 states that are XOR- ed to obtain the intermediate value
    - (04) Identity - considers value of intermediate state, results in 256 classes

Visualization

- provides an input gradient visualization feature
- allows the visual verification of main input samples learned from the input traces
- Input gradient can be visualized as:
  - (01) the sum of input gradients, providing the sum of input gradients computed for all used profiling traces and all the processed epochs
  - (02) the input gradient computed for all used profiling traces for each epoch in a heatmap plot.

Data Augmentation

- allows easy configuration of data augmentation techniques during model training
- allows small modifications in side-channel traces during training - improves the model generalization
- Implements two data augmentation techniques:
  (01) Shifts - every trace is randomly shifted
  (02) Gaussian noise - every trace is combined with the Gaussian noise with a specific mean and standard deviation values

Hyperparameter Search

- Two options to conduct hyperparameter tuning in the AISY framework
- Implements two data augmentation techniques:
    (01) Random search - need to define the minimal, maximal, and step value for every hyperparameter
    (02) Grid search - have to define all hyperparameter values to examine

Main Features of AISY framework

- SCA Metrics (guessing entropy and success rate)
- Gradient Visualization
- Data Augmentation
- Grid Search
- Random Search
- Early Stopping
- Ensemble

...contd

- Custom Callbacks
- Confusion Matrix
- Easy Neural Network Definitions
- Data Augmentation
- GUI - plots, tables
- Automatically generate scripts
- Fully reproducible scripts

Q & A

Thank You