Abstract

Transient Execution attacks are a computer/mobile device hardware attacks caused by the exploitation
of performance boosting techniques (e.g., branch prediction and speculation execution). Transient execution attacks are attacks that exploit transient executions, destined to be squashed. Year to year, a
variety of related transient attacks are flourishing. To address such kind of attacks, different mechanisms of detection and mitigation have been developed. Machine learning techniques are among the top ones to have been used to detect and classify transient execution attacks. Though deep
learning techniques such as Recurrent Neural Networks (RNNS), Convolution Neural Networks (CNNs) and Neural Networks based on back propagation are known to be effective, perceptron, a Neural Network based on a single layer is amenable to hardware design, fast to train, and fast for inference, thus fast in response to attacks.

This project is on the detection and classification of some transient execution attacks based on perceptron. The perceptron binary classifier is customized to build multi-class classifier. Dataset is collected using perf tool for the 302 performance counters. Python script is written to automatically dump data to text and then to comma separated values (csv) file.

The perceptron implemented was tested with the training data. Its accuracy is 100% for the training data. To test the inference accuracy, a dataset was collected from the same workloads and from the tweaked ones. Perceptron tuned out 100% accurate for the dataset collected from the same workload
and performed satisfactorily even for the dataset collected from the tweaked versions of the attack variants.