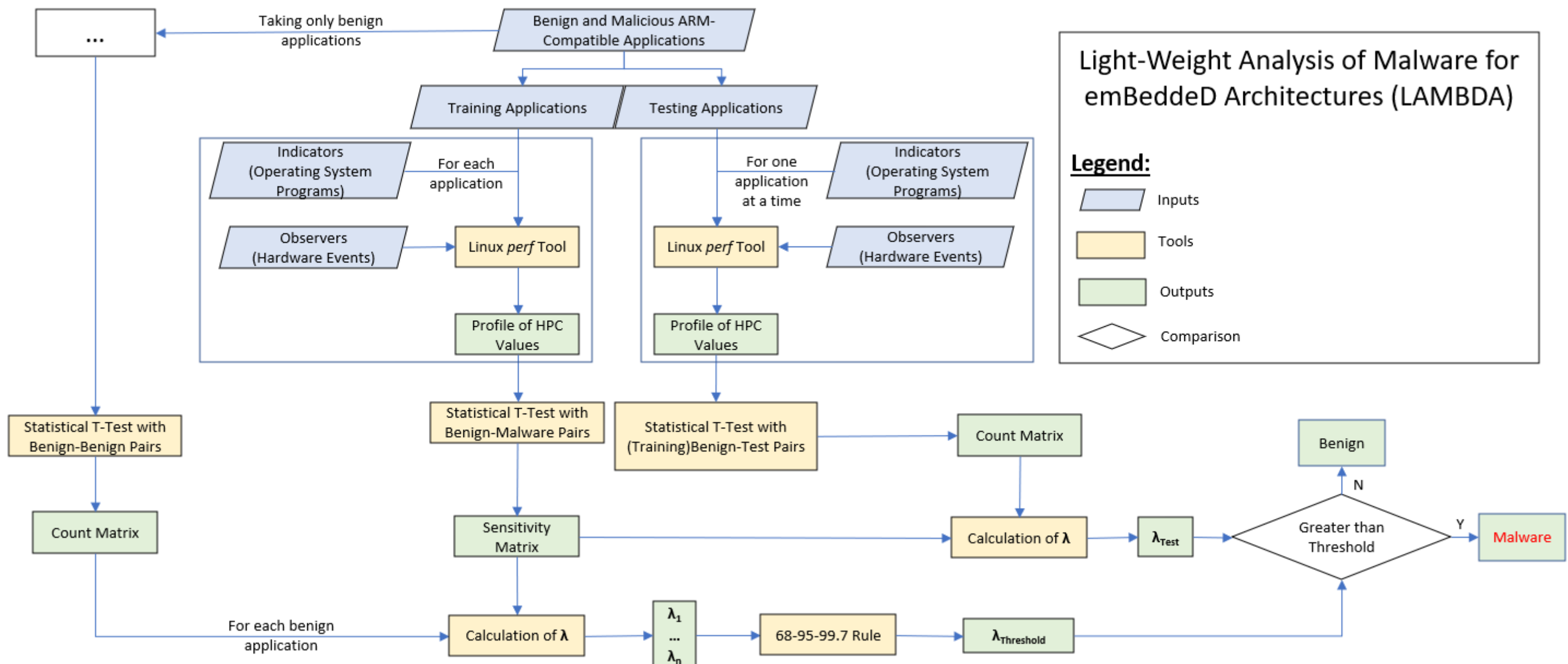


Hardware Assisted Malware Detection for Embedded Systems

Student: Willis Tee Teo Kian

Supervisor: A/P Lam Siew Kei



Project Objectives:

This project aims to create a lightweight malware detection prototype for embedded systems using Hardware Performance Counters (HPCs) as a metric for distinguishing benign and malicious applications. The prototype, Light-Weight Analysis of Malware for emBeddeD Architectures (LAMBDA), uses a statistical approach, T-Test, to quantify HPC values by estimating the true difference between two group means. By analyzing operating system programs (indicators) and HPC events (observers), HPC profiles for benign and malicious applications are generated and used for comparison.

Some Hardware Events:

1. Number of Instructions
2. CPU Cycles
3. Data Cache Access
4. Data Memory Access
5. Branch Predictions
6. Branch Mispredictions

Performance Monitoring Unit (PMU)

