Hardware Assisted
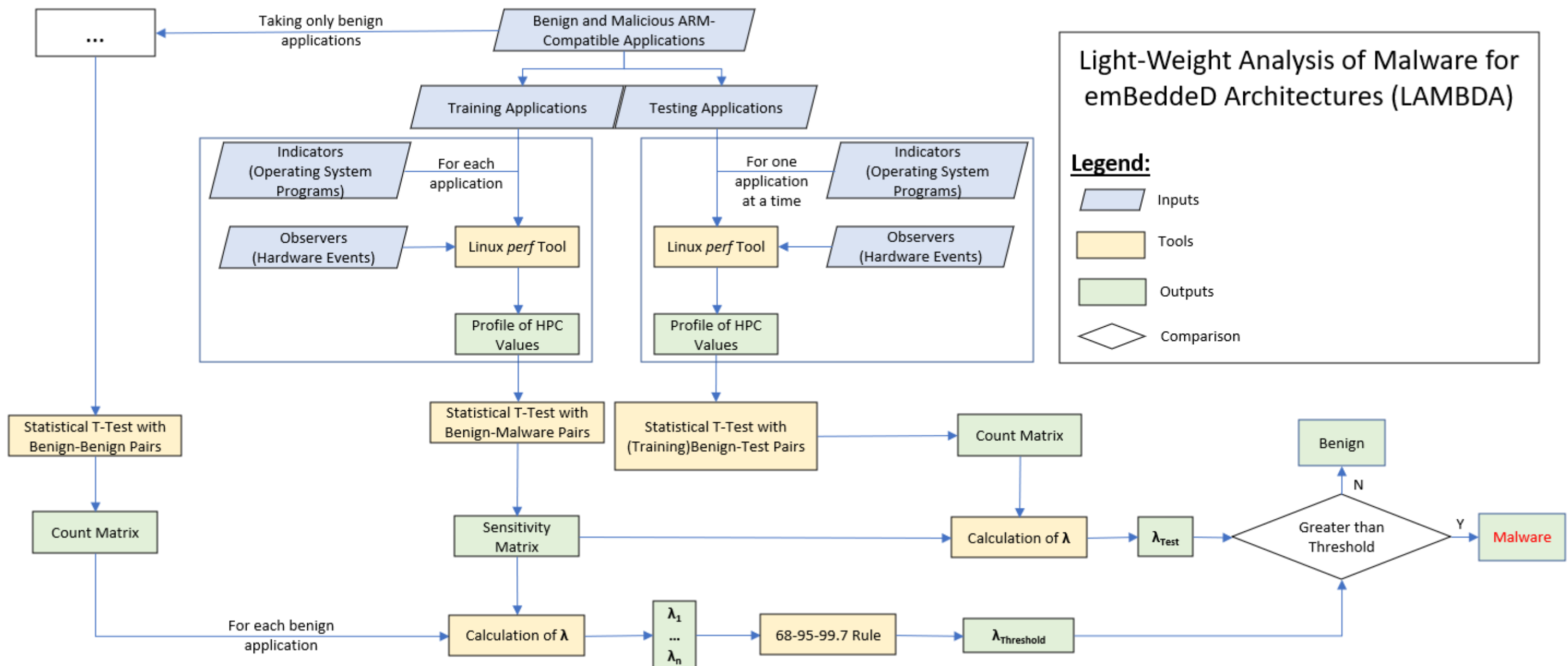## Malware Detection for Embedded Systems

Student: Willis Tee Teo Kian   Supervisor: A/P Lam Siew Kei

Taking only benign applications

...

Benign and Malicious ARM-Compatible Applications

Training Applications

Testing Applications

Indicators (Operating System Programs)

For each application

Observers (Hardware Events)

Linux *perf* Tool

Profile of HPC Values

For one application at a time

Indicators (Operating System Programs)

Linux *perf* Tool

Observers (Hardware Events)

Profile of HPC Values

Light-Weight Analysis of Malware for emBeddeD Architectures (LAMBDA)

Legend:

Inputs
Tools
Outputs
Comparison

Statistical T-Test with Benign-Benign Pairs

Count Matrix

For each benign application

Statistical T-Test with Benign-Malware Pairs

Statistical T-Test with (Training)Benign-Test Pairs

Count Matrix

Sensitivity Matrix

Calculation of λ

Calculation of λ

λ_{Test}

Greater than Threshold

N

Benign

Y

Malware

λ_1 ... λ_n

68-95-99.7 Rule

$\lambda_{Threshold}$

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)

CLKIN

Cycle Counter

System Control Processor/ APB interface

Count Enable Set/Clear Event Selection Registers

Performance Counter

Performance Counter

Events from other units

Performance Counter

Performance Counter

Interrupt/ Overflow registers

nPMUIRQ

Performance Counter

Performance Counter

Performance Counter