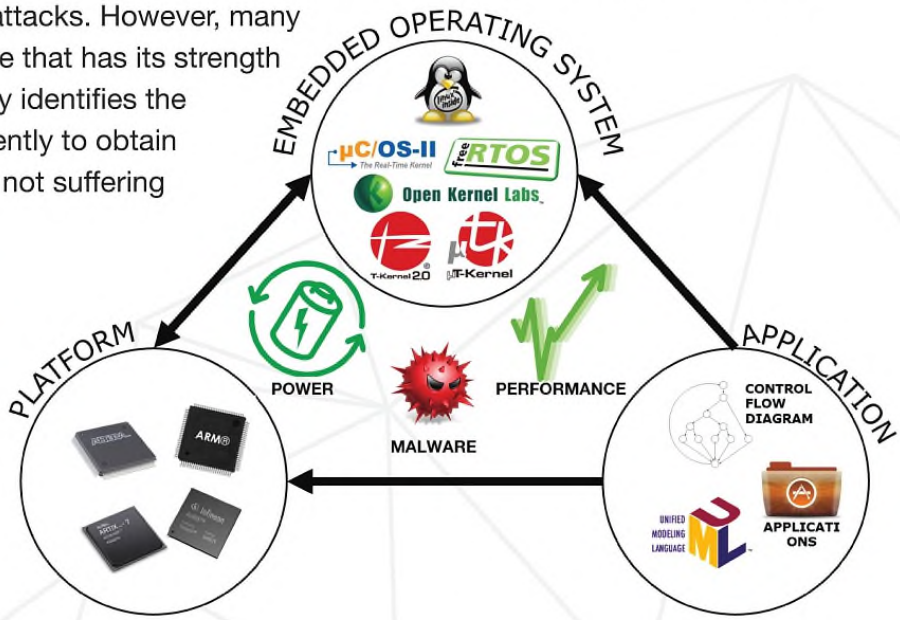
Multi Modal Approach to Anomaly Detection

Objective

To propose a light weight, yet robust framework for runtime anomaly detection in embedded systems. The framework should be capable of performing anomaly detection at multiple levels in the system, namely application, operating system and processor micro-architecture levels, by leveraging multiple features such as power consumption, system calls and hardware performance counters to ensure robustness.

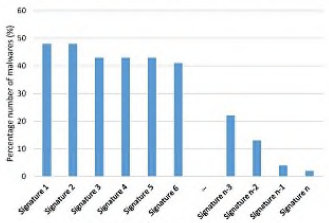
Proposed Anomaly Detection Approach

Existing intrusion detection techniques that could once detect malicious applications effectively, now fail, since they are unable to keep up with the rapidly evolving zero-day attacks. Currently, anomaly detection is a widely used technique to detect zero-day attacks. However, many existing methods focus on a particular feature that has its strength and weaknesses. The proposed methodology identifies the suitable features and combines them intelligently to obtain maximum advantages of their strength while not suffering from their individual weaknesses.

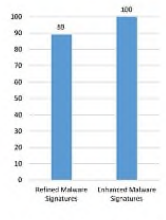


Work in Progress

System Call Based Signature for Malware Detection [ATIS 2017]

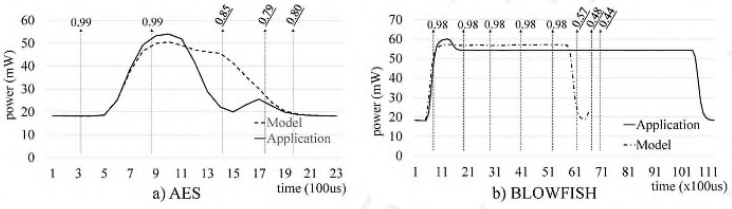


Sorted Malware Signature by percentage (% found in malwares)



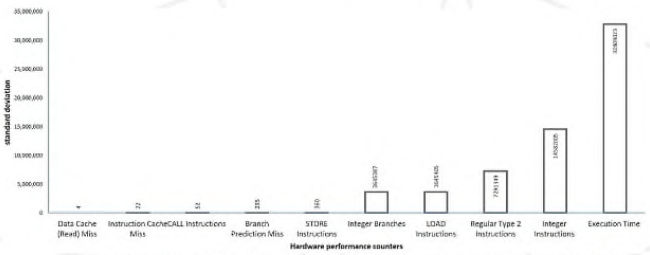
Sorted Malware Signature by percentage (% found in malwares)

Power Profile Based Anomaly Detection [TRON 2017]



Rapid runtime power analysis

Hardware Performance Counter Based Anomaly Detection [TRON 2017]



Averaged standard deviation of hardware performance counters cross twelve benchmark applications

Muhamed Fauzi, Alok Prakash and Thambipillai Srikanthan
School of Computer Science and Engineering
fauzi@ntu.edu.sg