Machine Learning for Embedded Security:

Identification and Mitigation of Side-Channel Attacks within the Internet of Things.

UNIVERSITY of LIMERICK
OLLSCOIL LUIMNIGH

Graham Claffey

Specialist Diploma in Embedded Systems Engineering

Introduction

With the increased demand of more powerful Integrated circuits and the need for internet connectivity within the IoT domain, we also need to ensure security can keep up with this rapid growth.

The recent raise in security threats known as side-channel attack has prompted more research in this area, with a lot of promising research and techniques demonstrated. In particular the main focus will be on detection and mitigation of cache-base side-channel attacks, with a light focus on other types.

Machine learning will be the key point on defending against these type of malicious attacks.

Aim

The main focus of this presentation is discussing how effective Machine Learning techniques are in detecting and also mitigating a various number of these side-channel attacks including:

- Timing attacks
- Differntial Power Analysis
- Electromagnetic attacks.

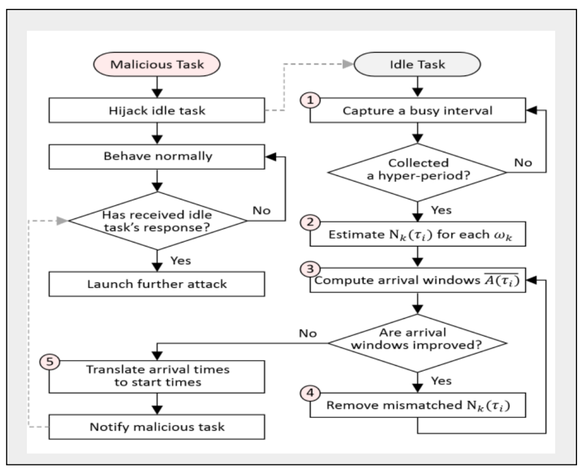
With the main focus being cache-based side-channel attacks.

Method

The methods used to undertake this project was to research the various types of side-channel attacks to gain a clear understanding of how they work, this was done with journal reading and online videos to get a visual demonstration of how the process of these attacks work. Some good resources are:

- Defcon – https://www.defcon.org/
- Liveoverflow - https://liveoverflow.com/
- BlackHat - https://www.blackhat.com/

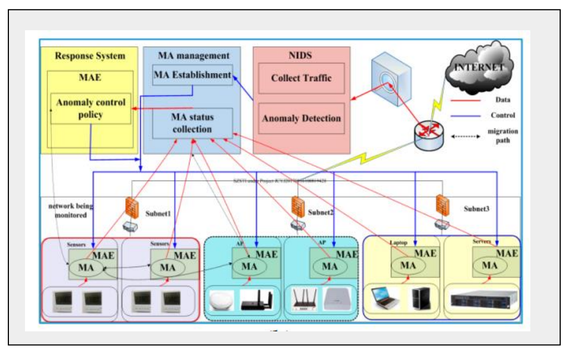
These were very valuable for live demonstrations and explanations of SCAs.



Attack flow of the proposed scheme between malicious task and idle task.,

Understanding the work on the machine learning side
Reading through various journals helped understand the current state and progression within this area. It allowed me to culminate the combined work from multiple researchers and gather an idea of how machine learning could help with security within the IoT.

There is some notable work currently being done in merging machine learning with IoT security. One that seems extremely promising is the Intelligent Maintenance and Lightweight Anomaly Detection System or IMLADS, were the anomaly detection system is trained with ML algorithms and operates on the network.



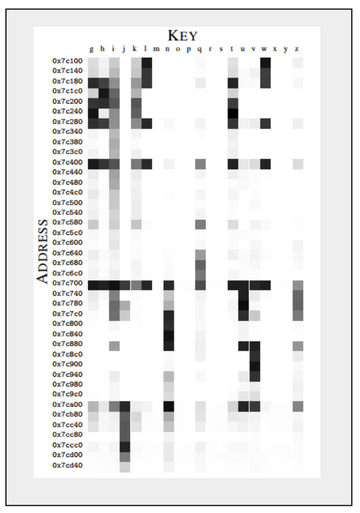
Introduction to Intelligent Maintenance and Lightweight Anomaly Detection System (IMLADS): framework of IMLADS.

Results

The results of the project shows that machine learning can be a very effective tool against SCAs. With some reported results as high as 99.51% detection rate within a test environment.

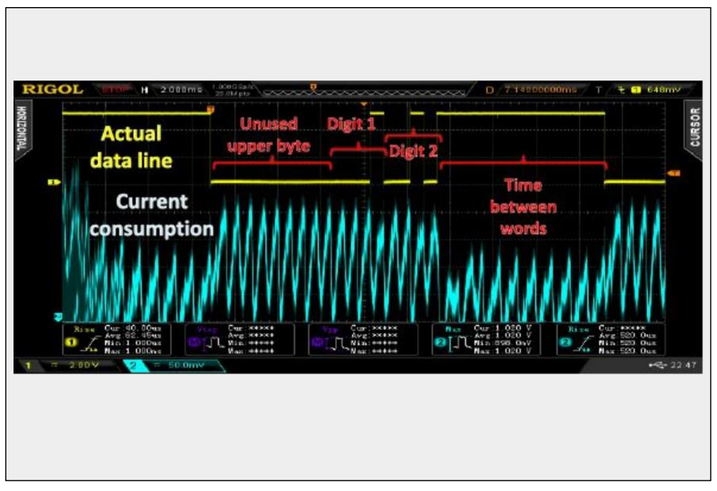
The regards to overhead on systems has also shown to be quite promising, where the overhead at runtime on some systems has show it to be 2% maximum.

The results have also shown that SCAs can be potentially very harmful. The main problem with SCAs is how adaptable they are to the current hardware architecture. Until more secure hardware architecture comes along, we seem to be stuck with SCAs.



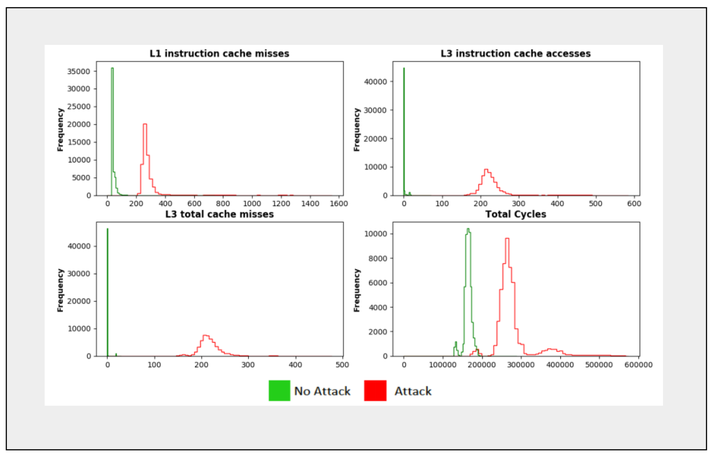
Excerpt of the GDK Cache Template. Dark ceels indicate key-address-pairs with high cache-hit ratios.

We can see from the research that machine learning has proven effective in detecting various red flags within a system that could indicate a side-channel attack is taking place. For instance with cache attacks, the cache hits and misses could be detected with the aid of ML.



Obtaining combination to Electronic safe lock using a timing attack to retrieve the correct digits from EEPROM.

Machine learning could help us detect and mitigate some of these issues until a more permanent solution is found.



Selected hardware events under Zero Load Conditions for RSA encryption algorithm: with and without Flush + Reload Attack.

Conclusion and personal reflection

The level of sophistication of side-channel attacks demonstrated on a wide variety of devices is an important reminder that we can never overlook the value of security within IoT.

I believe with machine learning implemented in every area of security, it can lead to an accurate and cost effective method to identify and mitigate similar threats that could arise from side-channel attacks. Rather than solutions of micro architecture overhauls of large performance impacts due to disabling hyper-threading.

Research into using machine learning on IoT devices is still in its infancy, the verity of approaches to solving these issues have made great progress and the research seems quite promising. It is these great steps that are needed to secure future IoT platforms.

E&CE | Department of Electronic and Computer Engineering