UNIVERSITY OF LIVERPOOL

Putting security at the very heart of every design...

STEM for BRITAIN

Security of Electronic Devices: Hardware Trojan Detection Through Machine Learning

Gor Piliposyan*, Saqib Khursheed | *PhD student, gor.piliposyan@liverpool.ac.uk

Introduction

What is a hardware Trojan (HT)?

Malicious inclusion or modification to the original design of the device to allow unauthorised access to the system to corrupt or retrieve secret information.

Where are these Trojans?

This research is concerned with detection of HTs on Printed Circuit Boards (PCBs) inside electronic devices.

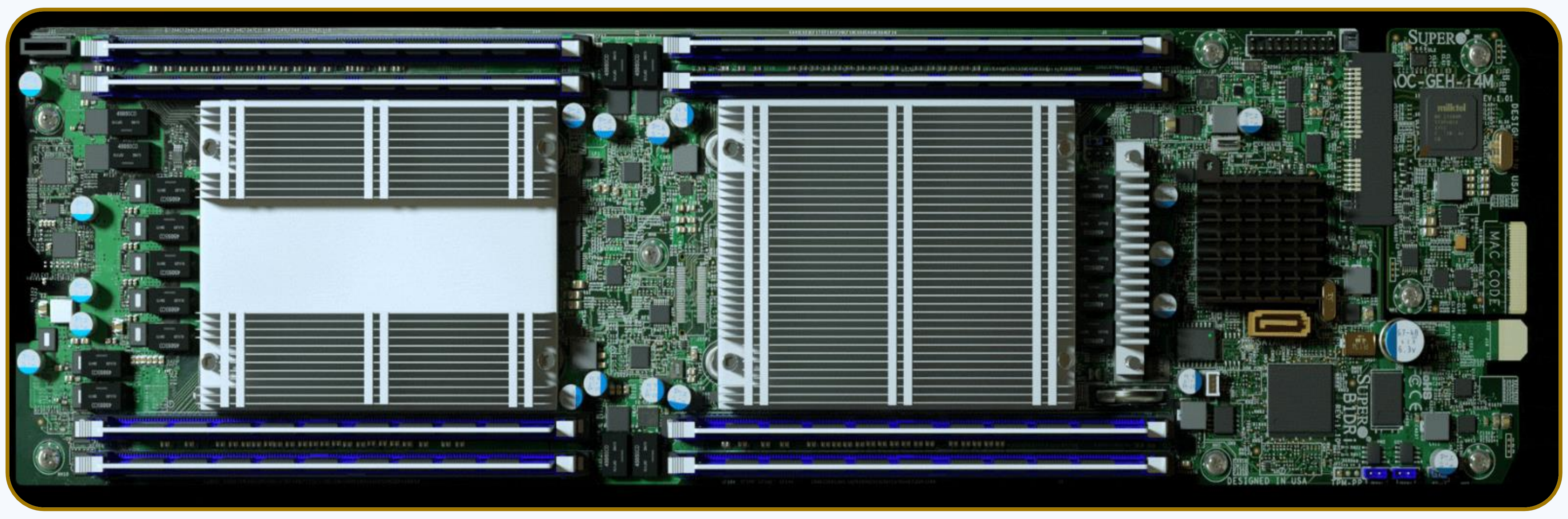
Why should we even consider HTs?

Given our dependence on electronic devices, HTs can have devastating impacts on modern society such as paralysing cloud services and financial systems.

How can we stop them?

By prospectively developing detection and prevention techniques. The cost of preventing a disaster is lower than recovering from it!

Trojan size visualisation



PCBs are integral parts of electronic devices used across multiple industries

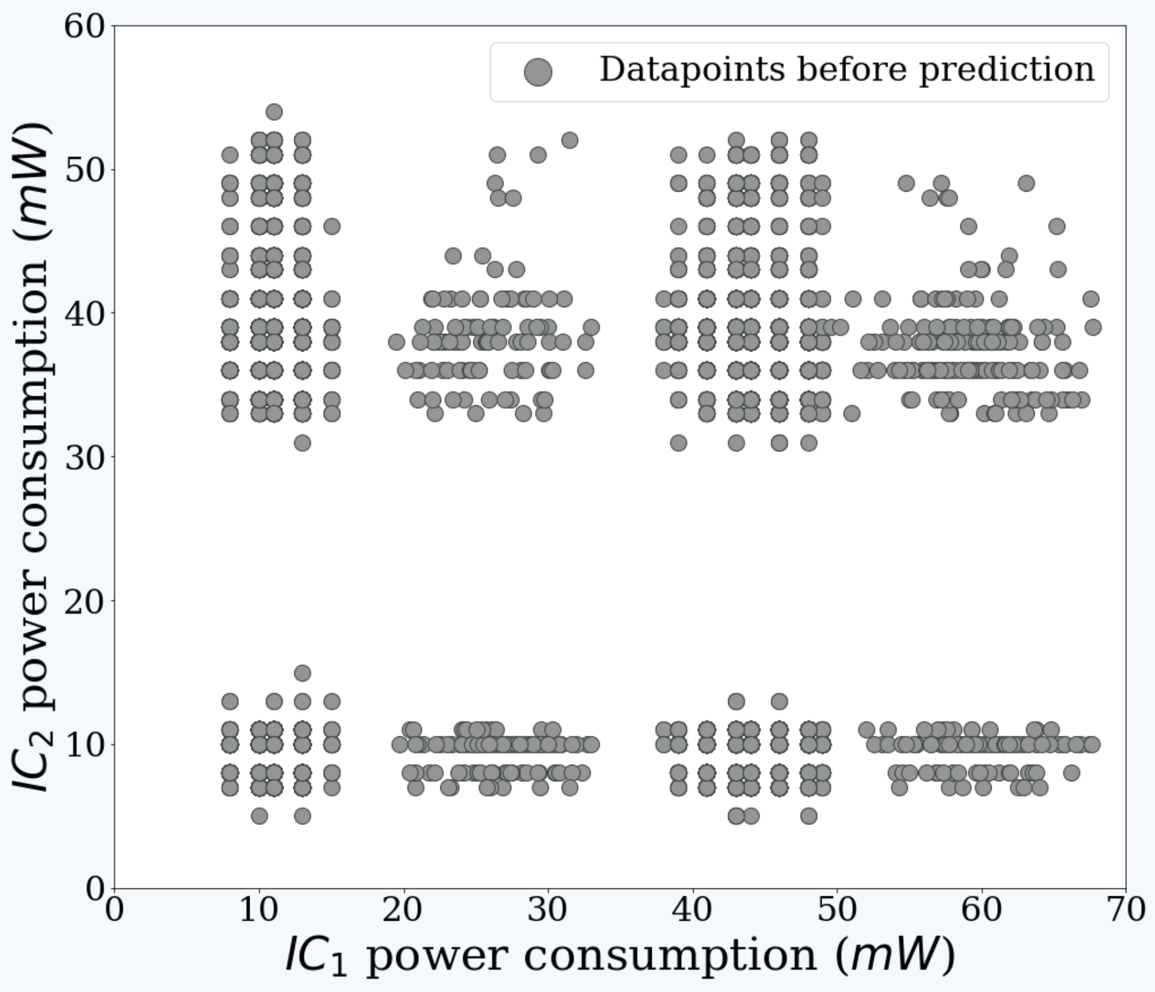
Trojan size visualisation

Methodology

Description: **I have developed a methodology that performs real-time detection of hardware Trojans on PCB's. Similar to how a doctor would check the heartbeat of a patient through electrocardiography for irregularities, my methodology monitors the PCB's power consumption pattern to identify anomalies. This is achieved by applying one class classification machine learning algorithms.**

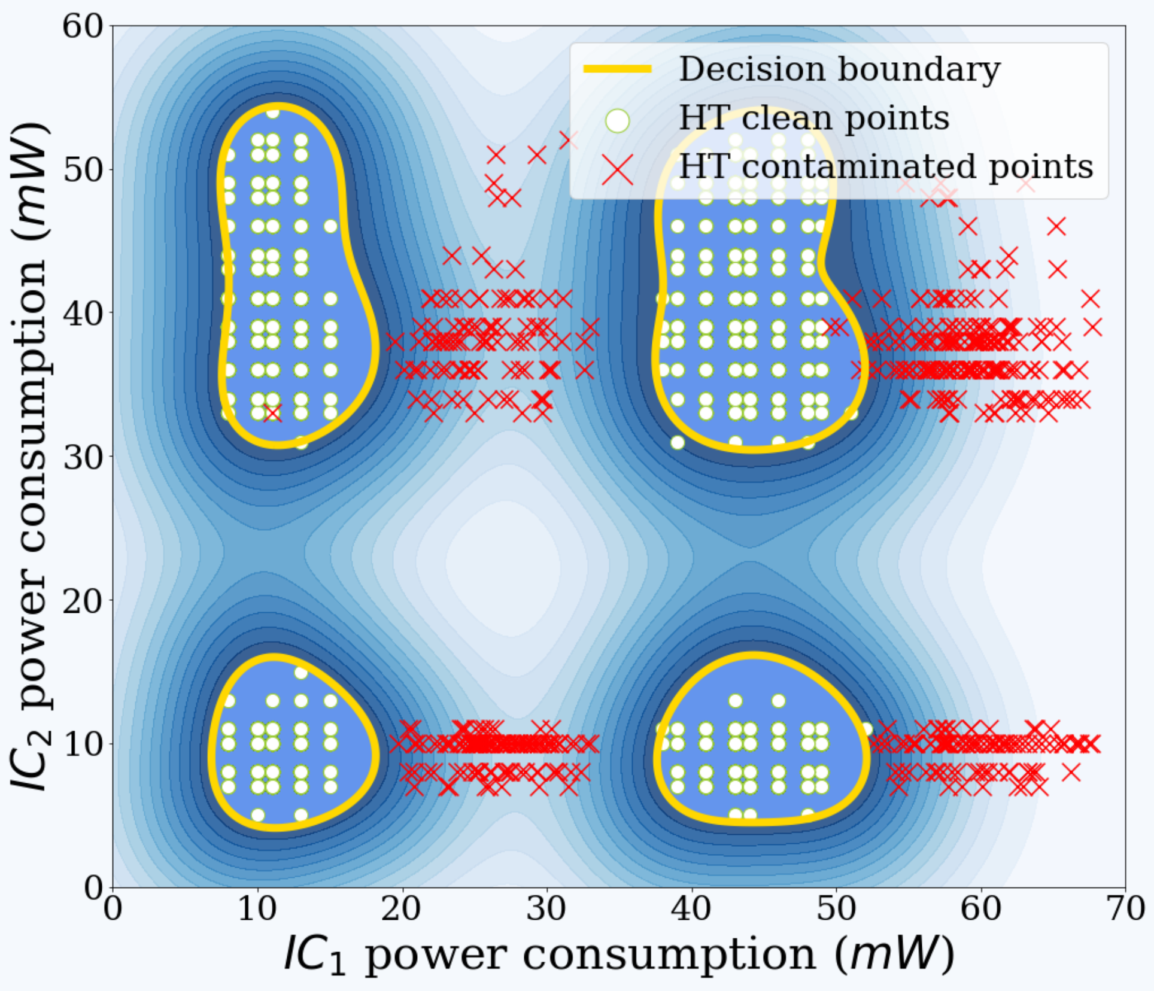
Task:

Separate Trojan infected datapoints from regular points.



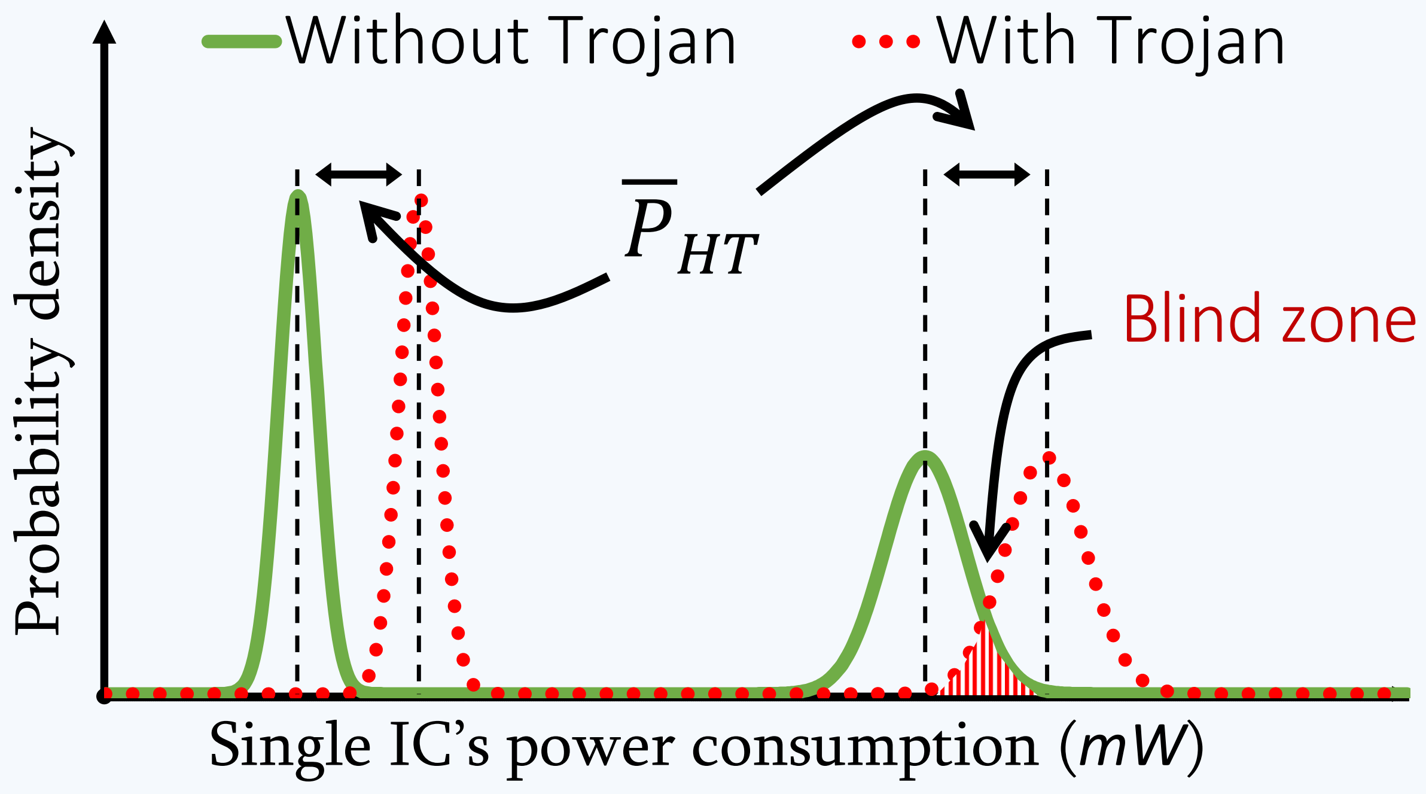
Solution!

Red points outside the decision boundary are labelled as Trojans.



But how?

Adding a Trojan on the PCB causes a shift in the anticipated power consumption curves.



Results: **Simulations returned HT detection classification results with an accuracy above 99.7% when the HT had an average power consumption as low as 40mW. The machine learning (ML) model is low-cost in terms of computation and memory, requiring as little as 20KB memory storage. Further, the simulation results have been validated through real-life experiments on a prototype PCB.**

Conclusion

This research targets hardware Trojans on printed circuit boards, an issue which has been proven to exist, but not sufficiently addressed. We proposed a power analysis method for detecting such HT components. We then applied ML techniques to detect stealthier HTs, powered from legitimate chips on the PCB. The results can have a significant impact in improving the level of electronic security, reducing the potential harm from HTs to society.

References

- G. Piliposyan, S. Khursheed, "PCB Hardware Trojan Run-time Detection Through Machine Learning", submitted to IEEE Trans. Emerging Topics in Computing.
- G. Piliposyan, S. Khursheed and D. Rossi, "Hardware Trojan detection on a PCB through differential power monitoring", IEEE Trans. Emerging Topics in Computing, doi: 10.1109/TETC.2020.3035521.
- www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies, last access 22/1/2022.

Though they are small and they are silent, make no mistake...
... for when awake, they fake and break!