Hardware Trojan Detection on a PCB Through Differential Power Monitoring

Gor Piliposyan
Dept Electrical Engineering and Electronics
University of Liverpool
Liverpool, UK
Gor.Piliposyan@liverpool.ac.uk

Saqib Khursheed
Dept Electrical Engineering and Electronics
University of Liverpool
Liverpool, UK
S.Khursheed@liverpool.ac.uk

Daniele Rossi
Dept Information Engineering
University of Pisa
Pisa, Italy
Daniele.Rossi1@unipi.it

***Abstract*—There is a general consensus that contemporary electronics are at risk of cyber-attacks or malicious modifications, such as Hardware Trojans (HT). This makes it crucial to develop reliable countermeasures at both Integrated Circuit (IC) and Printed Circuit Board (PCB) levels. While HT detection at IC level has been widely studied in the past several years, there is still very limited research carried out to tackle HTs on PCBs. We propose a power analysis method for detecting HT components implanted on PCBs. An experimental setup, using a hardware prototype, is built and tested for verification of the methodology, taking process and temperature variations into account. The results confirm the ability to detect alien components on a PCB and provide directions for further research. The performance degradation of the original PCB due to the implementation of the proposed approach is negligible. The area overhead of the proposed method is small, related to the original PCB design, and consists of Sub Power Monitors of individual ICs on the PCB and Main Power Monitor for the overall power measurement of the PCB. To the best of our knowledge this research is the first to develop a PCB HT detection methodology using power analysis.**

***Index Terms*—Hardware Trojan (HT), Printed Circuit Board (PCB), Power Monitoring, Trusted Manufacturing, Hardware Tampering Attacks and Protection, Hardware Prototype, Process Variation.**

I. Introduction

The rise of outsourcing of hardware fabrication to third parties in recent years has dramatically increased the possibility of malicious activities and consequently the security risk for systems incorporating the hardware. The harm to the system can be caused by destructive alterations and spy inclusions referred to as Hardware Trojans (HTs) [1], [2]. The HT is a rogue piece of hardware that is secretly deployed for a number of reasons, including information gathering, false signalling and control etc. Trojans can be inserted into an integrated circuit (IC) [3] or on a printed circuit board (PCB) and get control over data communication between, for example, the processor and the external components [4], [5].

The destructive activities of HTs can cause catastrophic consequences including paralysing major financial or military systems, shortening operational lifetime of the hardware or complete failure of the system [6]. HTs on a PCB or IC can give an attacker unauthorized access into the hardware and initiate a leakage or corruption of important information [7].

Hardware Trojans have become a serious problem in the last 10-12 years. There has been a dramatic increase in the number of publications since the original paper by Agrawal et al. in 2007 [10], where a novel side-channel based approach was proposed for detecting the presence of HT circuitry in ICs. Since then, research has been mostly focused on HT design, detection and prevention at IC level of abstraction [11]. The difficulty of detecting a Trojan is determined by its trigger and payload mechanism. Therefore significant research has been carried out on IC HT design and evaluation of new triggers and payloads [12]–[17]. Much more research however has been carried out on developing methodologies for IC HT countermeasures, which can be broadly classified as detection [8], [10], [18]–[20] and prevention [21]–[28] methods.

Malicious HT attacks have also been reported at higher levels of system abstraction such as PCBs, which are becoming increasingly exposed and vulnerable to unwanted modifications during design or fabrication in untrusted facilities [29]–[31]. Providing mechanical support for the electrical interconnections between different blocks, PCBs are an organic part of every electronic system. Modern complex and highly integrated designs may contain up to thirty layers with concealed micro-vias and embedded passive components [32]. An attacker can aim to modify the PCB design by tampering the interconnections or inserting extra components in an internal layer of a multi-layer board [7]. Like its IC counterpart, a PCB HT can serve two purposes, causing system failure or leaking secret information. A serious alarm on Hardware Trojan attacks on PCBs was raised by Bloomberg in 2018 [33], which reported on a very large-scale infiltration attempt into secret servers using a tiny malicious chip. The article alleged that the tampering attack on Super Micro servers affected around 30 companies, including US government contractors, a major bank, and other valuable companies. Although the Super Micro Computer company denied that malicious hardware chip has been implanted during the manufacturing process [34], it was demonstrated later [35] that such an attack is actually possible and feasible. Therefore developing countermeasures for HT detection on PCBs has become crucial [36]. This problem is addressed in the paper.

Prior Work: Very little research has been published concerned with countermeasures for PCB HTs. Amongst them [37] is concerned with an encryption and obfuscation based protection against HT risks on PCBs. This method requires the communicating chips to be equipped with encrypting and decrypting capabilities. Non-destructive board-level reverse engineering by x-ray imaging of a PCB is presented in [38]. This method, which allows extraction of all information required to reproduce the PCB, can be used to develop advanced countermeasures for PCB HTs. The rest of existing publications have been mainly concerned with security issues and post-fabrication tampering attacks [2], [29]. Since conventional PCB test methodologies often fail to detect PCB HTs [33], the importance of the problem and the gap in research make it crucial to investigate new countermeasures for detecting and preventing them.

The rest of the paper is organised as follows: the description of the attacker model in Section II is followed by the proposed approach in Section III. Then Section IV is devoted to the proposed methodology. Further, Section V describes the experimental setup with the results discussed in Section VI. Finally, the paper is concluded in Section VIII.

II. Attacker model

An HT implanted on the PCB can have different power sources, including: (a) a built in energy harvester/battery, (b) the mains supply, (c) the power distribution network (PDN) of the PCB and (d) an I/O pin of a legitimate chip. In case (a), a visual inspection of the board can lead to detection of the HT, since an energy harvester or a battery are typically large in size and hard to conceal. In order to connect to the mains power supply, the HT should have external vias which are visible, hence case (b) can also be detected through image processing and comparison with a golden model [38]. Of these cases, (c) and (d) are the stealthiest, since the HT can be fully operational, while all the modifications to the original design can be hidden in the internal PCB layers. In these cases an HT can escape detection through visual inspection, and research for alternative approaches is necessary.

In this attacker model it is assumed that the adversary can use any HT irrespective of its payload and trigger, as long as the malicious device consumes additional power. It is also assumed that the power to the PCB power distribution network goes only through the dedicated Main Power Monitor (MPM). Further, the IC and PCB design houses, as well as the firmware and intellectual properties used to design the ICs are trusted. The threat rises from outsourcing PCB production to overseas facilities, as well as from the possibility of interception while the device is in transit from the manufacturer to the consumer.

It is possible for the adversary to swap a trusted IC on the PCB with an HT infected and counterfeit (recycled, remarked) ICs, but this attack case is out of the scope of this paper. However, as mentioned in the introduction, there is a considerable amount of existing research aimed at design, detection and prevention of IC HTs and counterfeits [39]–[44], which can be utilised to tackle the threat of swapping ICs.

III. Our Approach

In this work, a Differential Power Monitoring (DPM) approach is proposed to detect Hardware Trojans on the PCB powered from the PDN. To the best of our knowledge, this is the first work on PCB HT detection using power monitoring. The approach is applied during in-field operation, as a run-time monitoring technique. Additionally, previous works can be used as complementary techniques (e.g. encrypting-decrypting communication between legitimate ICs [37]). Hardware Trojans are detected by measuring dynamic power due to HT circuit switching and static power due to HT leakage current. Continuous measurement of power consumption provides information on the PCB's internal activities and HT activation. It is assumed that the PCBs are not defective, therefore the source of any diversion from the expected power consumption patterns is assumed an HT.

The main characteristics of the proposed approach are:

1) **Independent of the type of Trojan:** Any HT that consumes power higher than the pre-programmed Detection Threshold will be detected.

2) **In-field, online monitoring:** This approach constantly monitors fluctuations in the power consumption of the PCB. It allows for in-field measurements and online monitoring.

3) **High accuracy:** False positive rate (FPR) can be reduced to virtually zero, depending on desired Detection Threshold.

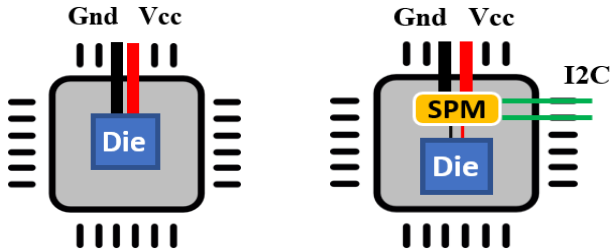
4) **Tolerance to Process and Temperature variations.**

5) **No interruption or performance overheads to the original performance of the circuit under monitoring:** The approach continuously monitors the PCB without interrupting the performance or affecting its throughput.

A similar approach for IC HT detection has been applied in [14] where the aim was HT detection prior to in-field use of the device. A current sensing resistor and an oscilloscope have been used to manually compute power consumption and detect the HT inside an FPGA. In our research a PCB integrated run-time HT detection framework has been implemented, where every legitimate IC has a dedicated digital power sensor.

Current integration method for detecting HTs inside ICs has also been suggested in [3] where the current consumption has been computed with a local sensor inside an IC. Using the current integration method, the data has subsequently been processed to detect HT induced anomalies. In our method, the difference between the readings from a global power consumption sensor and the sum of local power consumption sensors has been computed. This allows us to detect a Hardware Trojan implanted on the PDN that is located between the power source of the PCB and the legitimate ICs.

The approach proposed in this paper has been validated with experimental measurements. The results show that HT detection can be achieved with a low FPR while keeping the performance degradation at a negligible level and the area overhead minimal. Note that the end-users are required to carry out similar analysis based on their golden model and specific software workload scenarios. Similar to the case studies discussed in Section VI, Detection Thresholds can be decided using general guidelines provided later in this paper.



(a) (b)

Fig. 1: (a) Silicon die inside the package, (b) Sub Power Monitor and the die integrated into one package.

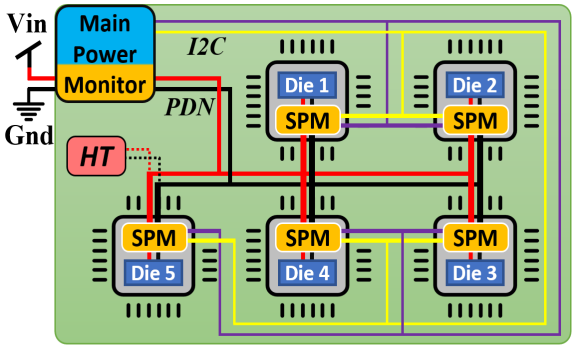


Fig. 2: Block structure of a PCB with the proposed Differential Power Monitoring system and a Hardware Trojan.

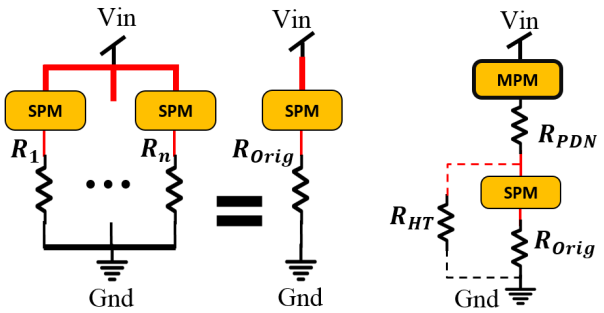
IV. Proposed Methodology

Regardless of the payload, trigger and the amplitude of the damage caused, one common feature of additional components introduced to a circuit is an increase in power consumption. The proposed DPM method is designed to detect extra power usage on the board. For a DPM to be feasible, the individual chips on the PCB should be equipped with power consumption sensors, henceforth referred to as Sub Power Monitors (SPMs) (Fig. 1).

The monitoring circuit consists of a main power monitor (MPM) device on the main power rail, and SPMs integrated with individual chips on the PCB (Fig. 2). The MPM includes a power sensor and a microcontroller for the noise dampening and data communication logic. The dampening logic takes the moving average of the readings from power sensors, while the communication logic acts as the device user interface.

As illustrated in Fig. 3a, the resistance of the original circuit on the PCB is formed by a parallel connection of multiple legitimate ICs. It can be summed up under one effective resistance (R_{Orig}). An HT device can be modelled as a resistive load (R_{HT}) added in parallel to R_{Orig} (Fig. 3b). When the HT is non-operational, it consumes little power and the value of its effective resistance is high. However, when the HT is triggered, its power consumption increases and this can be modelled by decreasing the value of R_{HT}.

In the case of an ideal power distribution network (PDN), it can be assumed that its power dissipation (P_{PDN}) on parasitic resistance is zero. If every component on the PCB has an



(a) (b)

Fig. 3: Abstraction of the (a) effective resistance of the original circuit, and (b) PCB with an added Hardware Trojan.

integrated SPM, the mismatch (ΔP) between the reading from the MPM (P_{MPM}) and the sum of the readings from SPMs ($\sum_{i=1}^{n}(P_{SPM})_i$) should be zero:

$$\begin{cases} P_{MPM} = \sum_{i=1}^{n}(P_{SPM})_i + P_{PDN} \\ P_{PDN} = 0, \end{cases}, \tag{1}$$

hence

$$\Delta P = P_{MPM} - \sum_{i=1}^{n}(P_{SPM})_i = 0. \tag{2}$$

However, real PDNs will naturally consume some power due to their non-zero parasitic resistance ($P_{PDN} \neq 0$). In addition, to account for the background noise, an extra term δ should be introduced into (2) and ΔP will be given as follows

$$\Delta P = P_{PDN} + \delta. \tag{3}$$

Furthermore, since every device has its dynamic and static power consumption, adding an HT component to the circuit will increase ΔP. The final sought after variable is

$$\Delta P_{HTinf} = P_{MPM} - \sum_{i=1}^{n}(P_{SPM})_i = \Delta P + P_{HT}^{Dyn} + P_{HT}^{Stat}, \tag{4}$$

where ΔP_{HTinf} is the mismatch between the total power consumption (P_{MPM}) and the sum of power consumptions by individual chips ($\sum_{i=1}^{n}(P_{SPM})_i$) on an HT infected PCB. The HT's dynamic and static power consumptions are represented by P_{HT}^{Dyn} and P_{HT}^{Stat}. Assuming the value of P_{PDN} is known for a given PCB layout, the existence of an inactive HT ($P_{HT}^{Dyn} = 0$) on the PCB can be detected through P_{HT}^{Stat}, if this value is considerably larger than δ ($P_{HT}^{Stat} >> \delta$).

On the other hand, it is also possible to detect a triggered HT through continuous monitoring. Once the triggering mechanism is activated, the internal states of the HT chip should switch to deliver the malicious payload. This inevitably introduces a sharp increase in the power consumption of the extra component represented as dynamic power consumption P_{HT}^{Dyn} in (4). In turn, the spike in P_{HT}^{Dyn} translates into a spike in ΔP_{HTinf} values (Fig. 4).

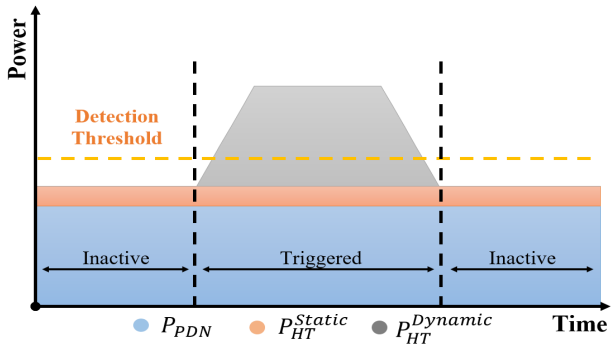


Fig. 4: Change in ΔP_{HTinf} when the HT is triggered.

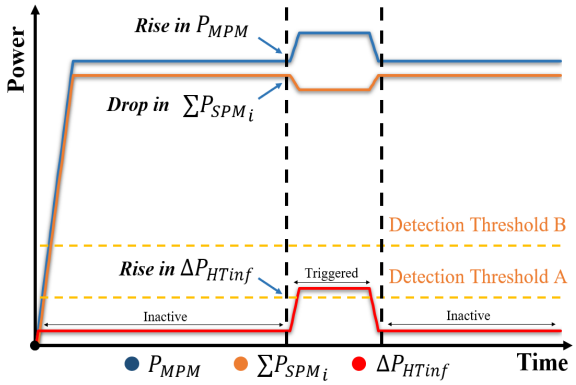


Fig. 5: Change in power consumption pattern when a Hardware Trojan is triggered.

In order to detect the HT based on increased ΔP_{HTinf} values, a new parameter is introduced - Detection Threshold (Fig. 4, Fig. 5). The choice of the Detection Threshold for a particular PCB is based on a number of parameters including maximum acceptable False Positive Rate and minimum detectable power consumption of the Hardware Trojan. Note that the Detection Threshold defines the highest value of ΔP_{HTinf}, above which anything is flagged as an active HT on the board. Its value is pre-programmed in the MPM block, taking into account the factors mentioned above.

In addition, along with the rise in the value of P_{MPM}, another characteristic feature of a triggered HT is the drop in $\sum_{i=1}^{n}(P_{SPM})_i$ which can be described by the following expression:

$$\Delta\sum_{i=1}^{n}(P_{SPM})_i = \sum_{i=1}^{n}(P_{SPM})_i - \left[\sum_{i=1}^{n}(P_{SPM})_i\right]_{Triggered}$$
$$= \frac{{V_{in}}^2}{R_{Orig}}\left[\left(\frac{R_{Orig}}{R_{PDN}+R_{Orig}}\right)^2 - \left(\frac{R_{new}}{R_{PDN}+R_{new}}\right)^2\right], \quad (5)$$

where $R_{new} = R_{Orig}R_{HT}/(R_{Orig}+R_{HT})$ and V_{in} is the input voltage. The power drop in (5), whose behaviour is schematically shown in Fig. 5, is due to the increased voltage drop on the PDN, after the Hardware Trojan has been triggered. The dependence of the drop in the combined SPM power consumption on R_{HT} is shown in Fig. 6 for three values of R_{PDN}. In this work, we have primarily focused on the spikes in ΔP_{HTinf} values, which take into account both the effect of the drop in $\sum_{i=1}^{n}(P_{SPM})_i$ and the rise in P_{MPM}, since ΔP_{HTinf} is the difference between them.

In order to reduce the background noise δ in (3), filtering by the moving average of every recorded ΔP_{HTinf} with its previous $N-1$ values is applied, where N (averaging level) is the number of averaged points. The resulting values are stored in a complementary $\Delta P_{HTinf}^{(N)}$ variable defined as

$$\Delta P_{HTinf}^{(N)} = \frac{\sum_{i=1}^{N}(P_{HTinf})_i}{N}.$$

Detectability trade-off between the HT activation time and power consumption should be considered since a higher averaging level N will result in a loss of accuracy in detecting

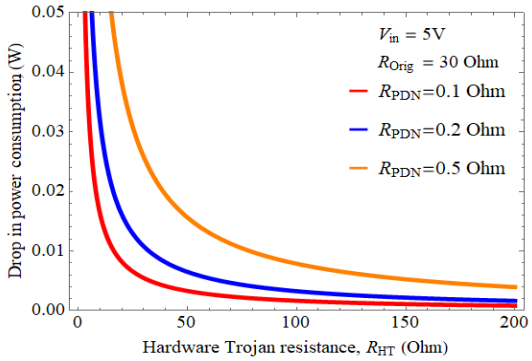


Fig. 6: The effect of R_{HT} on the drop in the registered combined Sub Power Monitor power consumption $\sum_{i=1}^{n}(P_{SPM})_i$.

short duration HT payloads, but will allow for detection of low-power HTs. The application specific optimal value for the averaging level N can be estimated from the following inequality

$$t_{HT} \geq N\frac{1}{\nu}, \quad (6)$$

where t_{HT} is minimum detectable HT activation time given as a technical requirement, and ν is the recording frequency of the monitoring system.

This technique successfully dampens the distortions introduced by the noise δ, as well as anomalies introduced through sensor error, which would otherwise be interpreted as peaks induced by an active HT (Section VI).

Detection Range Analysis

The Detection Threshold P_{thr} can be calculated using the following formula

$$\begin{cases} P_{thr} = \alpha\dfrac{|\delta_{\max}|}{N} + P_{PDN} \\ P_{SensRes} \leq P_{thr} \leq P_{HT}, \end{cases} \quad (7)$$

where N is the averaging level, P_{PDN} is the parasitic power consumption of the power distribution network, $P_{SensRes}$ is the power sensor resolution, and P_{HT} is the minimum value of the HT power consumption that we aim to detect. The

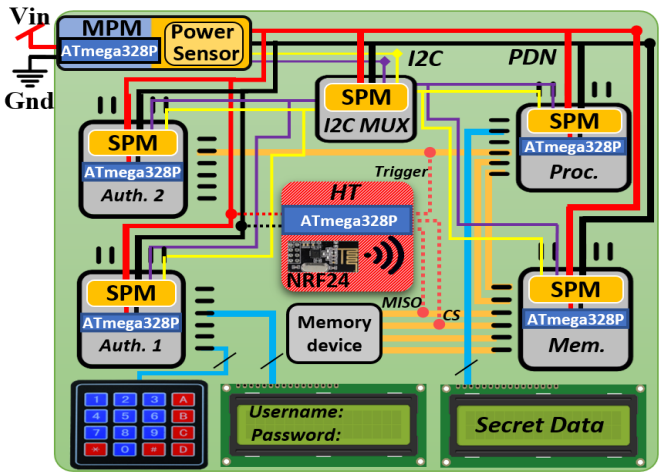


Fig. 7: Diagram view of the PCB prototype.

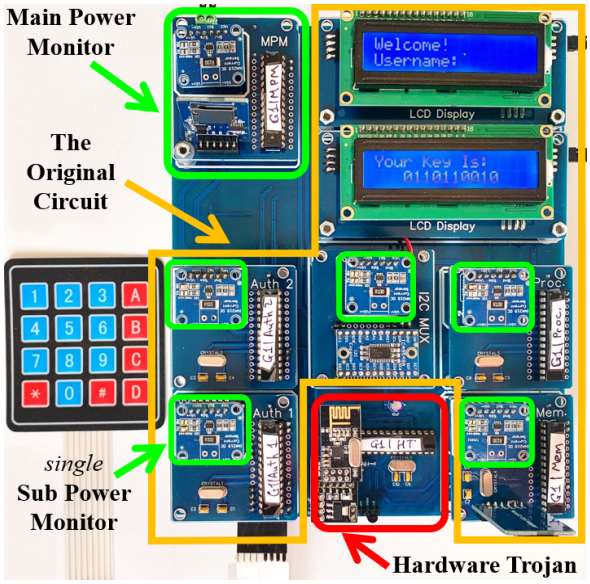


Fig. 8: Real life photo of the PCB prototype.

coefficient α ($\alpha \in (0, 1]$) can be determined experimentally on the given setup, once the value of the desired FPR has been chosen. For example, if it is required to have $FPR = 0\%$, then $\alpha = 1$. As for δ_{max}, it represents the maximum value of the background noise δ, which can be approximated by a normal distribution with zero mean.

It should be noted that the threshold is determined as a function of the amplitude of noise, the averaging level, and the power sensor resolution.

If n is the number of independent DPM outputs f_i ($i = 1, ..., n$), each of which has HT detection probability p, then f_i can be described as a Bernoulli distribution [45] with

$$f_i = \begin{cases} 0 & \text{HT not detected} \quad \Delta P_{HTinf} < P_{thr} \\ 1 & \text{HT detected} \quad \Delta P_{HTinf} \geq P_{thr}, \end{cases} \tag{8}$$

where ΔP_{HTinf} is defined in (4). It follows from (8) that the HT is detected when ΔP_{HTinf} reaches the HT Detection Threshold (7). If there is an active HT on a PCB, the maximum likelihood estimator for detection probability p for Bernoulli distribution (8) can be calculated as follows [45]

$$p = \frac{\sum_{i=1}^{n} f_i}{n}. \tag{9}$$

The detection probability (9) is proportional to the observed DPM outputs resulted in detection of the HT. It can be seen from (8) that this probability can be increased by decreasing P_{thr}, i.e. the detection probability also is a function of the same parameters as P_{thr}.

V. Experimental Setup

The original, Hardware Trojan free, circuit consists of four 16MHz ATmega328P microcontrollers which have been programmed and wired up into four blocks: Authentication (Auth. 1, Auth. 2), Processing, and Memory (Fig. 7, Fig. 8). Additionally, an I2C multiplexer, a keyboard and two displays have been integrated into the setup. The general function of the system is secret data transmission from the Memory block to one of the two integrated displays. Next, three different HT devices (Cases 1-3) have been introduced into the original circuit with the malicious purpose of data leakage. Finally, the proposed run-time Differential Power Monitoring circuit has been implemented on the setup.

A. The Original Circuit

The function of the original circuit (Fig. 8, shown by an orange border) is to store and display data from the built-in memory block, after a log-in procedure. A keyboard and a display, linked to the Authentication block, are leveraged to facilitate the log-in process. Upon a successful log-in event, an enable signal is generated by the Authentication block. This signal is fed into the Processing block. The enable signal triggers the Processing block to fetch the secret data from the Memory block. Here, the Processing block uses Inter-Integrated Circuit (I2C) communication protocol to request from the Memory block. In turn, the Memory block requests the data from a built in memory device through Serial Peripheral Interface (SPI). Once the secret data is passed to the Processing block, it is presented on a second display. The communication with both displays is executed through I2C protocol. After a pre-set time, the system automatically clears the displays and logs out, getting ready for a new log-in cycle.

B. The Hardware Trojan Device

HT Case 1: In this attack scenario the HT has three components: a 16MHz ATmega328P microcontroller, an NRF24L01 System-on-Chip 2.4 GHz radio frequency transceiver and a 5v/3.3v logic level shifter (shown in Fig. 7 and Fig. 8 with a red border). The device has five I/O pins: two power input and three data wires for timing the attack and eavesdropping on the interconnections on the original circuit. Two of the data wires are tapped to the SPI interconnections in

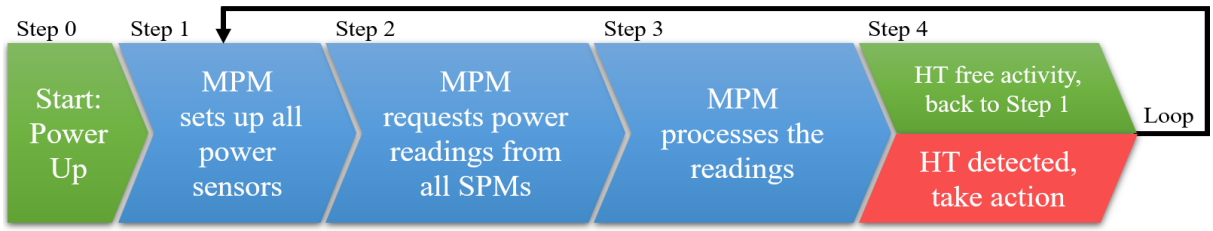


Fig. 9: The flow chart of Differential Power Monitoring logic steps.

Algorithm 1 Main Power Monitor data flow.

▷ **Step 0**
$P_{thr} := DetectionThreshold$ ▷ *Set Det. Threshold*
$N := AveragingLevel$ ▷ *Set Averaging level*
$\Delta P_{MovAvg}[\Delta P, N] := 0$ ▷ *Initialise moving average*
Initiate power sensors. ▷ **Step 1**
while 1 **do**
▷ *Storing data from sensors* | **Step 2**
$\mathbf{P_{MPM}} := sensor[0].GetPower$
for $i = 1, 5$ **do**
$\mathbf{P_{sumSPM}} += sensor[i].GetPower$
end for
▷ *Find new ΔP* | **Step 3**
$\mathbf{\Delta P_{new}} := P_{MPM} - P_{sumSPM}$
▷ *Update the moving average with new ΔP*
$\Delta P_{MovAvg}[\Delta P, N] := \Delta P_{MovAvg}[\Delta P_{new}, N]$
if $\Delta P_{MovAvg}[\Delta P, N] > P_{thr}$ **then** ▷ **Step 4**
Hardware Trojan detected.
end if
end while

the memory block. One of these wires carries a trigger signal, which turns the HT into an active transmitter, while the second wire is used to read the secret data. Additionally, a third wire is linked to the enable signal from the Authentication block. By default, the HT is set to sleeping mode to minimise the power consumption to stay undetected, and it only wakes up on a log-in event. To further increase its stealthiness, it is programmed to leak data after a certain number of log-in events. When the HT has reached the data leakage iteration, it powers on the radio-transmitter, which is otherwise turned off in order to reduce power consumption and avoid detection. Finally, the data is leaked out, and the HT device is sent back to sleep.

HT Case 2: To reduce the power consumption, we now consider an HT device with a 16MHz ATmega328P microcontroller unit. The HT has two states: 1) a state of active payload delivery after triggering, and 2) an idle state. The power consumption of the device in State 1 is around $5mW$-$10mW$, whereas in State 2 it is under $300\mu W$ (Power-Down mode). In Case 2, the payload of the HT is assumed to be arbitrary. The condition-based activation trigger for the HT can be either the enabling signal from the PCB circuit similar to Case 1, or an internal watchdog timer. The HT's pin connections are also executed in a similar way to Case 1.

HT Case 3: The always-on HT discussed in Case 3 is similar to the one in Case 2. A major difference, however, is in the operating pattern. As opposed to Case 2, here the HT does not have a triggering condition and is directly set to the only available active state after power up of the PCB. The power consumption of the device is in the range of $5mW$-$10mW$. In Case 3 the payload of the HT is assumed to be arbitrary. The pin connections of the HT, except for the trigger signal pin, are executed in a similar way to that in Case 1.

C. The Power Monitoring Circuit

There are two blocks to the power monitoring circuit: (a) a Main Power Monitor (MPM), and (b) five Sub Power Monitors (SPM) (Fig. 2, Fig. 7, Fig. 8 marked in green borders). Inside the MPM, along with the power sensor, an ATmega328P microcontroller has been used to conduct the on-board data processing and to deliver the dampening and communication functions. The microcontroller is linked to all power sensors via a multiplexer for communication using the I2C protocol. As illustrated in Fig. 9, after the initial power up (Step 0), the microcontroller in MPM sets up all the power sensors on the PCB (Step 1). Next, in Step 2 the MPM requests and receives power readings from all the sensors at a given time. Note that within one iteration the time-span between any two SPM readings is negligible. Then, in Step 3 it processes the obtained power readings. Finally, it follows from (8) that if the difference is larger than the pre-set Detection Threshold, an HT detection alarm is raised and the microcontroller begins the next iteration (Step 4). These steps are described in more detail in the form of the pseudocode Algorithm 1.

Power sensing is executed through INA219 high-side current and power monitor chips. These chips have a built in 12-bit ADC and provide readings with a resolution of 1mW.

VI. Experimental Results

The experiments performed support the theory described in Section IV. Three sets of experiments have been carried out. Firstly, as a proof of concept, the hardware prototype has been tested against three different HT attacks for detection capability assessment. Additionally, an HT detectability analysis has been carried out by dampening the noise level and finding the corresponding lowest threshold with 0% False Positive Rate (FPR). An experiment has also been set up to address varying and complex workload situations, which can induce an abrupt change in the power consumption of the legitimate board-level components. The purpose of this experiment is to validate the

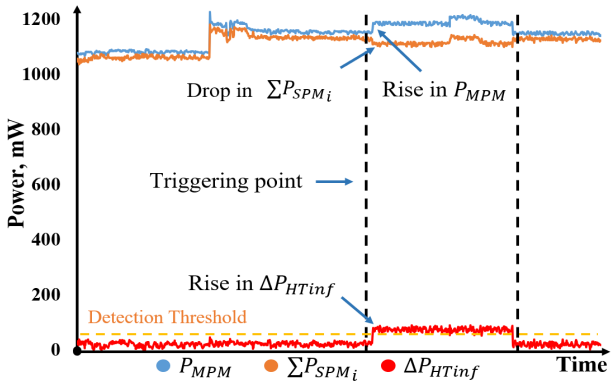


Fig. 10: Spike in ΔP_{HTinf} when HT is triggered, and drop in $\sum_{i=1}^{n}(P_{SPM})_i$ alongside the rise of P_{MPM}.

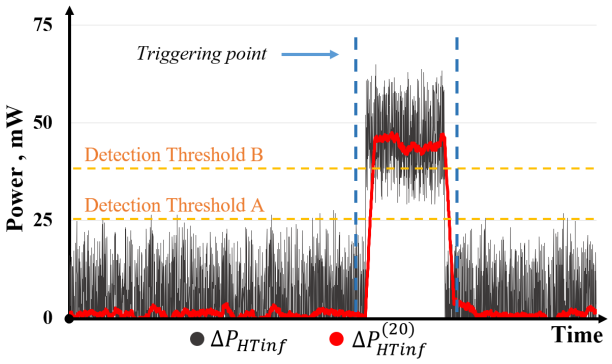


Fig. 11: ΔP_{HTinf} and $\Delta P_{HTinf}^{(20)}$ during HT triggering.

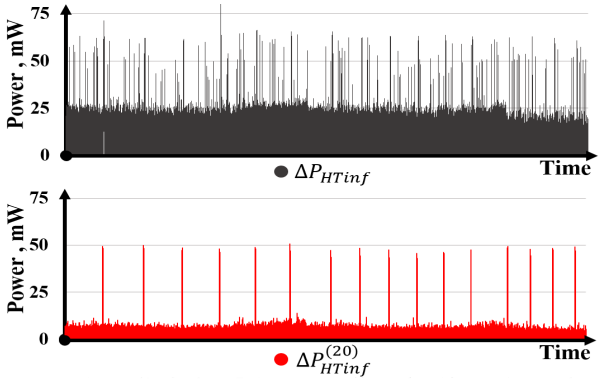


Fig. 12: Raw ΔP_{HTinf} (top grey graph), and $\Delta P_{HTinf}^{(20)}$ (bottom red graph) with an averaging of 20.

detectability of an HT on the PCB in a scenario where the legitimate ICs are running with varying workloads.

Secondly, ambient temperature variation experiments have been conducted to verify the robustness of the Differential Power Monitoring (DPM) methodology in a range of operating environments.

Lastly, the third group of experiments involved validation against process variation, where 5 groups of microcontrollers have been used to represent die-to-die variation.

A. *Proof of Concept and Averaging-Threshold Trade-off*

Data obtained from the experiments confirm the capability of the proposed DPM method to detect the presence of an HT on the PCB. The power values in Figs. 10-12 and Figs. 14-16, all functions of time, have been recorded with frequency ν of the monitoring setup and presented as time series, e.g.

$$\{\Delta P(t),\ t = \frac{n}{\nu},\ \nu = 100Hz,\ n = 1, 2, 3, ...\}. \qquad (10)$$

All experiments presented in this subsection have been carried out at room temperature (20°C).

HT Case 1: As illustrated in Fig. 10, there is a clear spike in ΔP_{HTinf} value, when an HT is triggered. If the value of this spike is larger than the pre-defined Detection Threshold, the HT will be detected. Note that as the Detection Threshold is lowered, lower power HTs become detectable. Two different Detection Thresholds are illustrated in Fig. 11. Here, level A provides a better HT detection resolution than level B, since it is capable of detecting lower ΔP_{HTinf} spikes. However, by lowering the Detection Threshold from B to A, the False Positive Rate increases due to the noise on ΔP_{HTinf} values.

Post-processing of the results of the measurements shows that applying a moving average filter greatly reduces the impact of noise on the raw ΔP_{HTinf} values (Eq. 4) as illustrated in Fig. 11 and Fig. 12. As can be seen in both figures, the $\Delta P_{HTinf}^{(20)}$ values produce a smoother signal with the averaging parameter set at $N = 20$.

One downside to this averaging technique is the risk of losing data on HT short-time scale activation, since the data may be smoothed in the same way as an anomalous peak. This issue can be addressed by introducing a higher frequency monitoring system, which is fast enough to record data several times while the HT is active. Ideally the monitoring system will sample the power readings of the PCB at least N times while the Trojan is active, where N is the number of data points used to calculate the moving average. The optimal value of N can be achieved through experimental means. On the other hand, the use of an averaging function creates a less noisy signal. As it can be seen in Fig. 11 the individual values of a noisy signal (black line) can be notably deviated from their average shown by the red line. By taking the moving average, these deviations are mostly alleviated. This allows us to detect an HT device drawing a lower amount of power. In addition, the moving average filtering provides significant improvements to the False Positive Rate (FPR) and the same values of FPR are reached at notably lower Detection Thresholds (Fig. 13). As shown in Table I, the minimum Detection Threshold for 0% FPR consistently drops along with the increase of the averaging level. For example, with the experimental setup

TABLE I: Detection Thresholds for $FPR \approx 0\%$

Time series	ΔP_{HTinf}	$\Delta P_{HTinf}^{(5)}$	$\Delta P_{HTinf}^{(20)}$	$\Delta P_{HTinf}^{(50)}$
Threshold	63 mW	20 mW	3.5 mW	1.9 mW

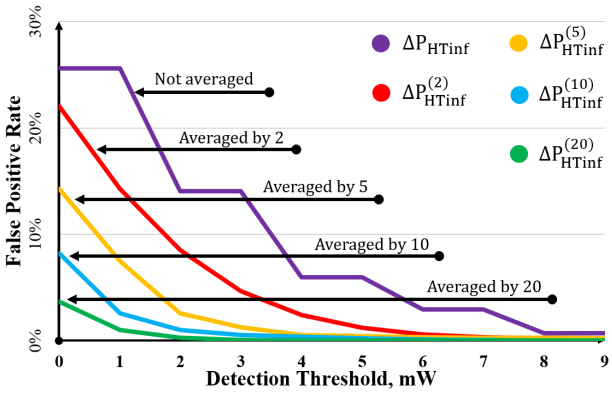


Fig. 13: False Positive Rate for 5 levels of averaging of ΔP_{HTinf} at room temperature.

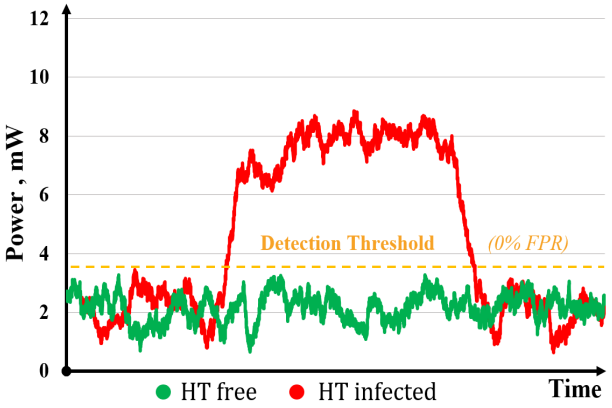


Fig. 14: Detection of a triggered Hardware Trojan; $\Delta P^{(20)}_{HTinf}$ at room temperature.

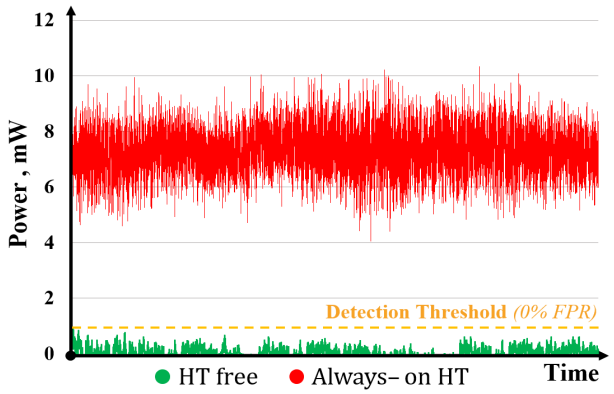


Fig. 15: Detection of an Always-on Hardware Trojan; $\Delta P^{(75)}_{HTinf}$ at room temperature.

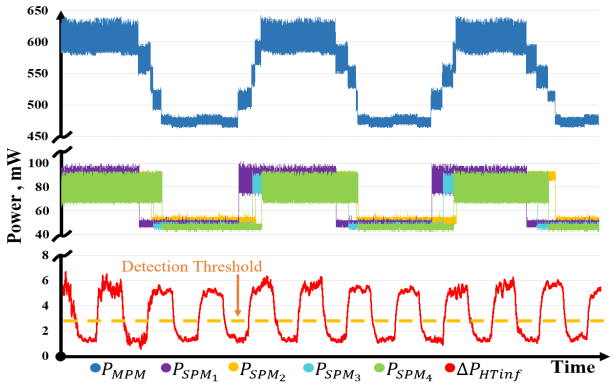


Fig. 16: Detection of a Hardware Trojan under variable workload of legitimate components.

under test, over thirty-fold reduction of Detection Threshold has been recorded for an FPR of zero percent, when the raw ΔP_{HTinf} $(63mW)$ values are compared to their moving averages $\Delta P^{(50)}_{HTinf}$ $(1.9mW)$ (Table I).

HT Case 2: In this case, described in Section V, a conditionally activated HT has been used for the attack. The results show that with a prior knowledge of the appropriate Detection Threshold $(4mW)$ the Hardware Trojan is easily detectable. As illustrated in Fig. 14 the power consumption of the activated HT (red line) fluctuates between $6mW$ and $9mW$. It can also be seen by the green line that the $\Delta P^{(20)}$ values from (10) fluctuate around $2mW$. The experiment has been repeated on a batch of 5 PCBs and the worst-case scenario PCB with the highest value of Detection Threshold for $FPR \approx 0\%$ has been chosen for illustration.

HT Case 3: In this case, an always-on HT has been used for the attack. The HT turns on when the PCB is powered on. As can be seen in Fig. 15, the moving average of the HT's power consumption (red line) was around $7.5mW$. Shown in green is the baseline PDN power consumption based on characterisation of a batch of HT free PCBs. It can be seen that by using a predefined Detection Threshold of 1mW it is possible to detect the HT with near 0% FPR. It should be noted that if the HT activation time is very long, as in the always-on case, the averaging level can be set to a high number (e.g. $N = 1000$) which will filter the noise down to the order of tens of μ-Watts. Hence, the HT power Detection Threshold (7) can be lowered to the same order.

Note that the proposed method uses different moving average filters to detect HTs with different characteristics (e.g. power consumption, active time). Depending on the targeted HT characteristics, one or more moving average filters may be deployed for optimal HT detection.

Variable Workload of Legitimate ICs: More complex situations with variable workloads of legitimate on-board components have been considered in this experiment. The Differential Power Monitoring method is used to detect the HT which has been programmed to switch on and off with a given time period and a consequent switch in power consumption from $7mW$ to less than $300\mu W$. As can be seen from Fig. 16, four legitimate ICs (P_{SPM1}-P_{SPM4}) change their power consumption at different times. This change is also clearly visible in the overall PCB power consumption (P_{MPM}). The results show that the power consumption of the HT (ΔP_{HTinf}) has been detected. As expected, it has repeatedly exceeded the predefined Detection Threshold despite the changes in the power consumption of the legitimate ICs.

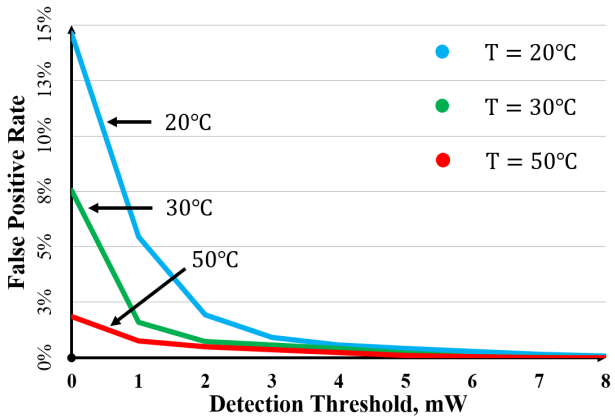


Fig. 17: Temperature variation effect on False Positive Rate.

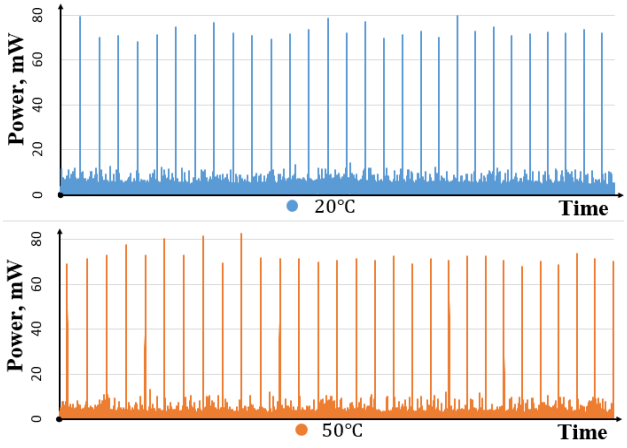


Fig. 18: $\Delta P^{(10)}_{HTinf}$ in 20°C and 50°C ambient temperatures.

B. Possible Attacks and Countermeasures

To further improve the proposed methodology it is crucial to understand how it can be circumvented. Two possible scenarios of an HT attack can be considered.

In the first scenario the adversary targets one of the legitimate IC and SPM module pairs. The communication wires between this victim SPM and the MPM module, as well as the power source wires of the legitimate IC are cut. Next, an HT with its dedicated fake SPM module is added under the same address name. Finally, both the HT and legitimate IC power are sourced through the fake SPM and it is connected to the MPM module. Now, whenever the MPM tries to read the victim SPM, it will actually address the fake SPM. This way the HT power consumption is added to the overall SPM measurements and is thus not detected. This attack can be counteracted by introducing existing HT prevention methods. For example, using cryptography as described by Z. Guo et al in [37] for the communication between the MPM and SPM modules can prevent the attack described above.

In the second scenario the HT is not powered from the power distribution network. An example of such an attack, where the HT is powered from an I/O pin of a legitimate IC, is mentioned in Section II. In this case the extra power consumption of the HT will be attributed to the legitimate IC and not contribute to ΔP_{HTinf}. Thus the HT will be invisible for the proposed monitoring system. Developing an algorithm based on characterisation of a batch of a given PCB design will help detect deviations from the expected power consumption pattern for each legitimate IC. Such deviations will indicate the presence of an HT device on the PCB. This approach will also address the first attack scenario discussed above.

C. Temperature Variation

Considering that real-life devices may be utilised in environments exhibiting different temperatures, it is necessary to verify the flexibility of Differential Power Monitoring (DPM) to adapt to a range of temperatures. To verify the capability of detecting power-consuming HTs, the developed hardware prototype has been tested inside a temperature chamber. As a case study this has been done for the attack scenario described in Case 1 (Section V-B). The results shown in Fig. 17 illustrate the reported FPRs in a range of temperatures (20°C, 30°C and 50°C).

Fig. 19: Temperature chamber.

According to these experimental results, the number of reported false positives drops significantly at higher ambient temperatures, with the lowest values in the experiment being at 50°C. This effect further strengthens the DPM method. Further, the experiments have been repeated 5 times at every temperature and the HT was successfully detected in every case. A representative view of $\Delta P^{(10)}_{HTinf}$ values (including the HT's power consumption spikes) at 20°C and 50°C is given in Fig. 18. When comparing the results, it can be seen that no notable change was recorded in the peak values of $\Delta P^{(10)}_{HTinf}$. Based on this evidence, the chances of detecting an HT device on the PCBs are higher at higher ambient temperatures.

The equipment used to conduct the experiments is a Gallenkamp hot box oven with a fan, model OV-165 with an error margin of +/- 1.5° Celsius (Fig. 19).

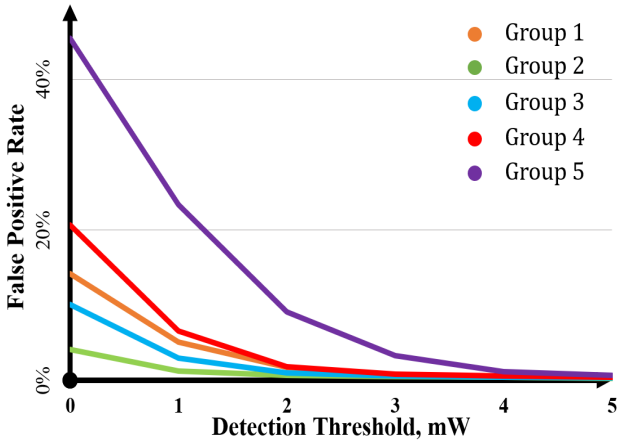


Fig. 20: Process variation effect on False Positive Rate for microcontroller groups 1, 2, 3, 4, and 5 at room temperature.

D. Process Variation

In recent semiconductor devices ($< 90nm$) the effect of process variation cannot be ignored. Fabrication process variation is mainly due to sub-wavelength lithography, random dopant distribution, line edge roughness and stress engineering [46], [47]. It has been shown that more than 30% difference in the drive current of a transistor is observed on a 65-nm device due to process variation, when compared to the nominal operating condition [47]. Process variation has negative effect on the quality of manufacturing test as well, leading to test escapes [48]. It can be further categorised into Intra-die (die-to-die) and Inter-die (within die) variation. The experiments conducted in this research address die-to-die process variation.

The proposed DPM method requires knowledge of the power consumption patterns of the PCB in order to determine the optimal Detection Threshold, therefore, a characterisation stage of a PCB batch is required. To account for process variation effects across the batch, the same experiment has been conducted with five groups of microcontrollers (Group 1, 2, 3, 4, and 5), five times each. As a case study this has been done for the attack scenario described in Case 1 (Section V-B). The Main Power Monitor (MPM), Authentication, Processing and Memory blocks in the original circuit as well as the HT (Fig. 7) were swapped with a new set of chips and observed for detection of any changes in the functionality of the power monitoring block. With the averaging parameter set at $N = 10$ ($\Delta P^{(10)}_{HTinf}$), the experimental results, illustrated in Fig. 20, show large variations of FPR at lower Detection Thresholds. However, the FPR registered a sharp fall at higher Detection Thresholds ($> 5mW$). Even in the worst-case scenario (Group 5) the FPR was below 1% at the Detection Threshold of 5mW. With the Detection Threshold set at 13mW, the FPR was zero in all five cases. All experiments explained in this subsection have been carried out at room temperature (20°C).

VII. Limitations and Future Work

The detectability of HTs can be affected by issues that are beyond the scope of this paper.

A. Detectable HT Payload Delivery Time and Power

The recording frequency of the DPM monitoring setup in our prototype is around $\nu = 100Hz$. This sets the threshold of the minimum detectable activation period of an HT at about $10ms$. HTs with longer activation periods will be recorded, as long as the overall power consumed by the HT is higher than the Detection Threshold. Note that the power sensors used in our prototype are limited to a relatively slow I2C (up to 2.56 Mbps $High\text{-}speed$ mode) communication protocol. The results can be significantly improved by leveraging faster communication protocols.

It is clear that even lower power HTs can be detected by changing the monitoring equipment and introducing higher frequency and more accurate sensors with better resolution and precision. For example, using INA226 digital power senors with a resolution of $10\mu W$ (ADC 16bits) will decrease the lower limit of Detection Threshold 100 times compared to the prototype discussed in this paper.

B. Statistical Analysis and Theoretical Underpinning

The detectability of HTs is also affected by issues including the RC characteristics of the PCBs' wires, and workload dependent drift in the parasitic power consumption of the PCB's power distribution network. Even in a noise-free environment, and assuming ideal precision and speed of power sensors, these effects provide a window of opportunity for the adversary to implant a very small HT device and avoid detection. The theoretical underpinning with statistical analysis of the proposed work will be considered in our future work.

VIII. Conclusion

This paper is the first to develop a methodology on detecting Hardware Trojan (HT) components on a Printed Circuit Board (PCB) using power monitoring. The methodology proposed here is independent of the HT's trigger and payload functions. The presented results show that the proposed Differential Power Monitoring (DPM) method, based on power consumption, can detect HT devices implanted on the PCB, with a false positive rate (FPR) that can become zero by selecting appropriate Detection Threshold (Table I). Considering the diversity of operating conditions in real life scenarios, the DPM has been validated in a temperature chamber for temperature variation. In addition, process variation factor has also been considered, which plays a crucial role in sub-90nm technologies. In particular, five different groups of microcontrollers have been employed to extract hard-silicon process variation data.

The Differential Power Monitoring (DPM) technique provides additional protection for end users without affecting the throughput of the PCB. It can be employed in conjunction with other PCB HT countermeasures without cross-disruption. Key variables in the DPM technique that can be improved upon are

sensor frequency, resolution and accuracy, and the averaging level for ΔP_{HTinf}. The proposed methodology can be further improved by using more sophisticated sensors, communication protocols and carrying out theoretical underpinning as described in Section VII. This along with other improvements will be considered in our future work.

ACKNOWLEDGMENT

This project was funded in part by the Department of Electrical Engineering and Electronics, University of Liverpool, UK and by the Italian Ministry of Education and Research (MIUR) in the framework of the CrossLab project (Departments of Excellence), Department of Information Engineering, University of Pisa. The authors of the paper also thank the anonymous reviewers for their constructive suggestions.

REFERENCES

[1] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, "Trustworthy hardware: Identifying and classifying hardware trojans", Computer (Long. Beach. Calif), pp. 39–46, 2010.

[2] Y. Jin, E. Love and Y. Makris, "Design for Hardware Trust" Introduction to hardware security and trust, Chapter 17, M. Tehranipoor and C. Wang, Eds., Springer New York, pp 365-384, 2012.

[3] X. Wang, H. Salmani, M. Tehranipoor, and J. Plusquellic, "Hardware Trojan detection and isolation using current integration and localized current analysis", Proc. IEEE Int. Symp. on Defect and Fault Tolerance in VLSI Systems, pp. 87-95, 2008.

[4] V. Jason, " Introduction to Hardware Trojans" The hardware Trojan war: Attacks, myths, and defenses, Chaper 2, S. Bhunia and M. M. Tehranipoor, Eds. Spring Int. Publ., pp.15-51, 2018.

[5] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection", IEEE Design and Test of Computers, vol. 27 pp. 10-25, 2010.

[6] A. Iyengar and S. Ghosh, "Hardware Trojans and Piracy of PCBs" The hardware Trojan war: Attacks, myths, and defenses, Chap. 6, S. Bhunia and M. M. Tehranipoor, Eds. Spring Int. Publ., pp.125-145, 2018.

[7] S. Ghosh, A. Basak, and S. Bhunia, "How secure are printed circuit boards Trojan attacks?", IEEE Design & Test, vol. 32(2), pp. 7-16. 2015.

[8] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware trojan attacks: Threat analysis and countermeasures", Proc. IEEE, vol. 102(8), pp. 1229-1247, 2014.

[9] H. Li, Q. Liu, and J. Zhang, "A survey of hardware Trojan threat and defense", Integr. VLSI J., vol. 55, pp. 426-437, 2016.

[10] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, and B. Sunar, "Trojan detection using IC fingerprinting", Proceedings IEEE Symposium Security and Privacy, pp. 296-310, 2007.

[11] R. S. Chakraborty, S. Narasimhan, and S. Bhunia, "Hardware trojan: Threats and emerging solutions", Proc. IEEE Inter. High-Level Design Valid. and Test Workshop, HLDVT, pp. 166-171, 2009.

[12] C. Dunbar and G. Qu, "Designing trusted embedded systems from finite state machines", ACM Trans. Embed. Syst., 13(5s), pp. 1-20, 2014.

[13] Y. Shiyanovskii et al., "Process reliability based trojans through NBTI and HCI effects", NASA/ESA Conference on Adaptive Hardware and Systems, pp. 215-222, 2010.

[14] X. Zhang, K. Xiao, M. Tehranipoor, J. Rajendran, and R. Karri, "A study on the effectiveness of Trojan detection techniques using a red team blue team approach", Proceedings IEEE VLSI Test Symp., pp. 1-3, 2013.

[15] L. Lin, W. Burleson, and C. Paar, "MOLES: Malicious off-chip leakage enabled by side-channels", IEEE/ACM International Conference on Computer-Aided Design, Digest of Technical Papers, pp. 117-122, 2009.

[16] B. Cha and S. K. Gupta, "A resizing method to minimize effects of hardware trojans", Asian Test Symposium, pp. 192-199, 2014.

[17] N. G. Tsoutsos and M. Maniatakos, "Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation", IEEE Trans. Emerg. Top. Comput., vol. 2(1), pp.81-93, 2014.

[18] K. Xiao, X. Zhang, and M. Tehranipoor, "A clock sweeping technique for detecting hardware trojans impacting circuits delay", IEEE Des. Test, vol.30(2), pp. 26-34, 2013.

[19] D. Forte, C. Bao, and A. Srivastava, "Temperature tracking: An innovative run-time approach for hardware Trojan detection", IEEE/ACM Int. Conf. on Computer-Aided Design, Digest of Technical Papers, ICCAD, pp. 532-539, 2013.

[20] B. Zhou et al., "Detecting Hardware Trojans using backside optical imaging of embedded watermarks", Proceedings Design Automation Conference, pp. 1-6, 2015.

[21] J. B. Wendt and M. Potkonjak, "Hardware obfuscation using PUF-based logic", IEEE/ACM International Conference Computer-Aided Design, Digest of Technical Papers, ICCAD, 2015.

[22] A. Baumgarten, A. Tyagi, and J. Zambreno, "Preventing IC piracy using reconfigurable logic barriers", IEEE Des. Test Comput., vol. 27(1), pp. 66-75, 2010.

[23] R. P. Cocchi, J. P. Baukus, L. W. Chow, and B. J. Wang, "Circuit camouflage integration for hardware IP protection", Proceedings of the IEEE Design Automation Conference, 2014.

[24] K. Xiao and M. Tehranipoor, "BISA: Built-in self-authentication for preventing hardware Trojan insertion", Proc. of the IEEE Int. Symp. Hardware-Oriented Security and Trust, vol. 1, pp. 45-50, 2013.

[25] K. Vaidyanathan, B. P. Das, E. Sumbul, R. Liu, and L. Pileggi, "Building trusted ICs using split fabrication", Proc. IEEE International Symposium. Hardware-Oriented Security and Trust, pp. 1-6, 2014.

[26] B. Hill et al., "A split-foundry asynchronous FPGA", Proc. of IEEE Custom Integrated Circuits Conference, pp. 1-4, 2013.

[27] Y. Xie, C. Bao, and A. Srivastava, "Security-aware design flow for 2.5D IC technology", Proc. of the 5th Int. Workshop Trustworthy Embedded Devices, co-located with CCS, 2015.

[28] J. Valamehr et al., "A 3-D split manufacturing approach to trustworthy system development", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 32(4), pp. 611-615, 2013.

[29] K. Rosenfeld and R. Karri, "Attacks and defenses for JTAG", IEEE Des. Test Comput., vol. 27(1), pp. 36-47, 2010.

[30] A. Hennessy, Y. Zheng, and S. Bhunia, "JTAG-based robust PCB authentication for protection against counterfeiting attacks", Proc. Asia and South Pacific Design Automation Conf., ASP-DAC, 2016.

[31] S. Paley, T. Hoque, and S. Bhunia, "Active protection against PCB physical tampering", International Symposium on Quality Electronic Design, ISQED, pp. 356-361, 2016.

[32] W. Jillek and W. K. C. Yung, "Embedded components in printed circuit boards: A processing technology review", International Journal of Advanced Manufacturing Technology, vol.25(3-4), pp. 350–360, 2005.

[33] "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", 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 22/8/2020.

[34] www.supermicro.com/en/news/CEO-letter, last access 22/8/2020.

[35] media.ccc.de/v/35c3-9597-modchips_of_the_state, last access 22/8/2020

[36] D. Mehta et al., "The Big Hack Explained: Detection and Prevention of PCB Supply Chain Implants", ACM Journal on Emerging Technologies in Computing Systems, vol. 16(4), 2020.

[37] Z. Guo, X. Xu, M. M. Tehranipoor, and D. Forte, "EOP: An Encryption-Obfuscation Solution for Protecting PCBs Against Tampering and Reverse Engineering", Cryptogr. Secur., Submitted 2019.

[38] N. Asadizanjani, M. Tehranipoor and D. Forte, "Non-destructive PCB reverse engineering using X-ray micro computed tomography", IEEE Transactions on Components, Packaging, and Manufacturing Technology, pp. 292 - 299, 2017.

[39] U. Guin et al., "Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain", Proc. of the IEEE, vol. 102(8), pp. 1207-1228, 2014.

[40] A. L. H. Martinez, S. Khursheed and D. Rossi, "Leveraging CMOS Aging for Efficient Microelectronics Design", IEEE 26th International Symposium on On-Line Testing and Robust System Design, 2020.

[41] D. Rossi, V. Tenentes, S. Khursheed, S. Reddy, "Recycled IC Detection through Aging Sensor", European Test Symposium, 2018.

[42] Tehranipoor et al., Counterfeit Integrated Circuits: Detection and Avoidance, Springer, 2015.

[43] D. Rossi, V. Tenentes, S. Yang, S. Khursheed and B. M. Al-Hashimi, "Reliable power gating with NBTI aging benefits", IEEE Transactions on Very Large Scale Integration Systems, 24(8), pp. 2735–2744, 2016.

[44] A. Stern et al., "EMFORCED: EM-Based Fingerprinting Framework for Remarked and Cloned Counterfeit IC Detection Using Machine Learning Classification", IEEE Transactions on Very Large Scale Integration Systems, vol. 28(2), pp. 363-375, 2020.

[45] Sheldon M. Ross, “Introduction to Probability and Statistics for Engineers and Scientists”, Elsevier, 624p, 2014.
[46] D. Reid et al., “Analysis of threshold voltage distribution due to random dopants: A 100,000-sample 3-d simulation study”, Electron Devices, IEEE Transactions on, vol. 56(10), pp. 2255 –2263, 2009.
[47] W. Zhao et al., “Rigorous extraction of process variations for 65-nm CMOS design”, Semiconductor Manufacturing, IEEE Transactions on, vol. 22(1), pp. 196–203, 2009.
[48] U. Ingelsson, B. Al-Hashimi, S. Khursheed, S. Reddy, and P. Harrod, “Process variation-aware test for resistive bridges”, Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on, vol. 28(8), pp. 1269–1274, 2009.

Gor Piliposyan received the B.S. degree in Radio-Physics and Electronics from Yerevan State University, Yerevan, Armenia. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, U.K. His research interests are in the areas of hardware oriented security of low-power designs and machine learning.

Saqib Khursheed received the Ph.D. degree in electronics and electrical engineering from the University of Southampton, Southampton, U.K. He is currently a Lecturer (Assistant Professor) with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, U.K. He is interested in addressing challenges related to hardware oriented security, green computing, reliability, and testability of low-power designs, and 3-D integrated circuits. He has authored a number of papers in internationally leading journals and conferences in these areas.

Daniele Rossi received the MSc degree in electronic engineering and the Ph.D. degree in electronics and computer engineering from the University of Bologna, Bologna, Italy, in 2001 and 2005, respectively. He is currently an Associate Professor in Electronics with the Department of Information Engineering, University of Pisa, Italy. His current research interests include hardware security, energy efficient and reliable digital design, and robust design for soft error and aging resiliency. Dr. Rossi has co-authored over 100 papers published in international journals and conference proceedings, and holds one patent.