Cooling Power Waste Evaluation Resulting from Malicious Thermal Measurements in Multicore Processors

Michael Kausch, Andrew Ibrahim, Mostafa Abdelrehim
California State University, Bakersfield, CA, USA
Emails:{mkausch, aattia-ibrahim, mabdelrehim}@csub.edu

***Abstract*—Security attacks on thermal sensors cause the improper reporting of hardware temperatures. This can lead to a decrease in the lifetime of hardware and also an unnecessary increase in power consumption. These security threats due to the presence of malicious thermal sensors can significantly increase energy consumption of cloud computing data centers e.g. Amazon cloud, Microsoft Azure, etc. This poster paper examines the excess power consumption that results from the improper reporting of thermal readings on a Raspberry Pi which can be used to model cloud computing centers in a small scale fashion.**

***Index Terms*—Multicore Processors, Hardware Trojan, Thermal Sensing**

I. Introduction

Data Centers have high energy requirements under normal operations. Some of the world's cloud computer centers require ≈100MW to work efficiently which is enough to power 80,000 US homes [1]. A report by the Environmental Protection Agency estimates that in 2006, 61 billion kilowatt-hours (kWh) or roughly 1.5% of total U.S. electricity consumption was attributed to data center energy consumption.

In a review of data center best practices, Greenberg and associates placed particular emphasis on efficient cooling strategies [2] which can reduce the total power consumption anywhere from 33% to 50% [2]–[4]. A coordinated cooling method locally at the processors and centralized at the data center is undertaken to optimize cooling energy consumption [5, 6]. When the embedded cooling power is not enough to overcome individual processor heat, the centralized cooling power increases accordingly [5] which of course increases energy cost.

Data Centers have the ability to hold billions of megawatts of important information. Everyone across the globe uses data and in turn that data is stored inside a data center. The issues that might arise with CPU temperatures rising could end up being heavy capital cost and permanent data loss as well [7]. This could definitely hinder the peak capacity for performance by throttling the CPU or causing faster wear out to the components as well as causing potentially irreversible damage to the components [7]. This study is performed to show how much power and money could be saved if a Data Center is secured, however, if a Trojan does exist we display the damage that a Trojan could have as an impact in efficiency in Data Centers.

Dynamic Thermal Management (DTM) techniques are used to maintain local cooling [8] which relies heavily on CPU thermal sensors to properly report an accurate temperature. As DTM directly relies on thermal sensors, the accuracy and trustworthiness of thermal sensors are key factors. In this paper, we address the situations at which a thermal sensor is maliciously or benignly not functioning properly. This may happen due to either i) having unwanted modifications in the sensor circuit design in order to facilitate future security attacks (also known as Hardware Trojan) [9] or ii) permanent or transient faults occurrences in the sensor or its accompanying circuitry [10]. A malfunctioning thermal sensor would simply report $t \pm \Delta t_{error}$ where t is the actual temperature of the core and Δt_{error} is the error injected by the infected rouge sensor. That may either cause performance degradation by, for example, asserting unnecessary frequency throttling by the DTM or accelerate aging processes reducing the lifetime of the chip. In this paper we study the situation in which a rouge sensor would report $t + \Delta t_{error}$ in which case extra cooling power would be triggered by the central cooling system to overcome the false increase in heat causing unnecessary energy waste.

The remainder of this paper is presented accordingly, section II will detail the methods used to analyze the problem. Section III will show the results of the research methods. Finally, Section IV concludes the paper.

II. Methods

A. Materials

A Raspberry Pi 4 (RPi) was used to model a one server data center. Two TKA United brand Power Meters were used to measure the power output of an Amazon Basics brand desk fan and the RPi (Fig. 1). The fan was then connected to a Digital Power Relay which was then connected to the RPi's GPIO pins. This setup necessitated that one of the sides of the RPi case be removed and exposed the SoC. The fan was

controlled by the Raspberry Pi using the GPIO pins modulated by an in-house kernel written in C++.

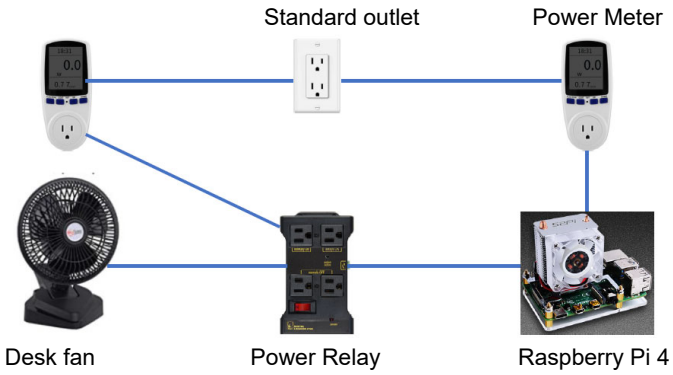


Figure 1: Example Test Setup.

The controlling program was written such that each of the four cores of the RPi CPU were kept under load at near 100% utilization while monitoring the CPU temperature as reported by the thermal sensor. Testing began if and only if the temperature of the CPU is at ambient temperature (was ≈52°C inside the chip). The fan was activated during the test if the program reported that the CPU temperature had reached a predetermined threshold ($t_{threshold}$). The fan was deactivated during the test if the CPU temperature had fallen below $t_{threshold}$. The soonest the fan could cycle on or off was 10 seconds from the last time it was previously cycled on or off.

During "normal" conditions, baseline power consumption was measured and the reading from the thermal sensor was unaltered. In order to assess the effects of a malfunctioning thermal sensor, Δt_{error} was added to the actual temperature measurement t during the "attack" conditions. The effect that Δt_{error} had on power consumption was assessed by testing Δt_{error} to be either $10°C$ or $15°C$.

The fan was kept on the lowest setting. The displacement that the fan was from the RPi varied from 1ft, 2ft and 3ft distances. Power readings were then taken at 10 second intervals for either 10 minutes or 30 minutes tests.

B. Analysis

The power associated with the Raspberry Pi and the fan were summed together to create one data point for the power of the system. Cumulative Power Consumption for each one minute period was calculated by summing the power until that time period. Total power consumption was then used to calculate the % increase in power usage. This data can be found in Table I.

C. Effect of Δt_{error}, $t_{threshold}$, Distance and Time on % Increase in Power Waste

Total power consumption as well as the % increase in power consumption was calculated and can be found reported in Table I.

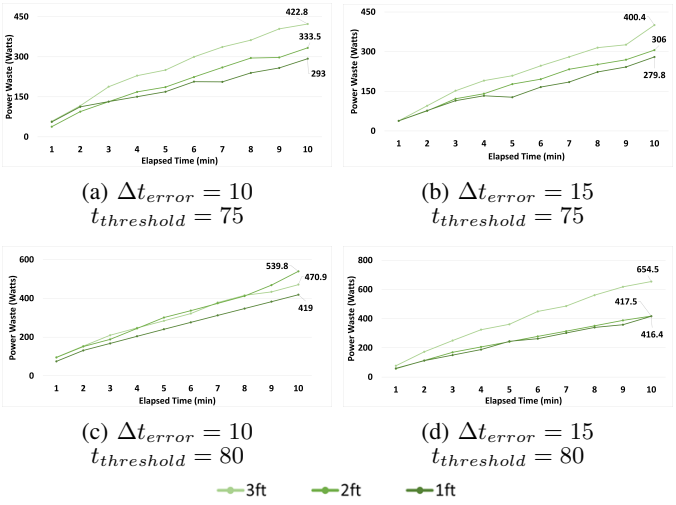
Table I: % Power Increase by Testing Condition

Parameters				Total Power (W)		% Increase in
Δt_{error}	$\Delta t_{threshold}$	Dist (ft)	Time (min)	Normal	Attack	Power
10	75	3	10	692.8	1115.6	61.03%
10	75	2	10	650.6	984.1	51.26%
10	75	1	10	651.3	944.3	44.99%
10	80	3	10	678.5	1078.9	59.01%
10	80	2	10	636.8	942.8	48.05%
10	80	1	10	576.5	856.3	48.53%
15	75	3	10	710.8	1181.7	66.25%
15	75	2	10	636.2	1176	84.85%
15	75	1	10	654.3	1073.3	64.04%
15	80	3	10	707.3	1361.8	92.53%
15	80	2	10	640.4	1057.9	65.19%
15	80	1	10	538.7	955.1	77.30%
10	80	3	30	1026.5	2574.4	150.79%
10	80	2	30	1026.5	1841.3	79.38%
10	80	1	30	1026.5	1874.5	82.61%

Power Waste was then calculated by subtracting the "normal" condition from the "attack" condition. Scatter plots were then created comparing the distances for each test condition, with each test condition varying Δt_{error} and $t_{threshold}$ (Fig. 2). The total power waste was noted on the graphs for the final data point.

Average Power consumption was calculated as a way to compare the overall power use. All data points were summed to calculate the Total measured power during the test and average power was calculated by dividing by the total number of readings taken (Fig. 3).

III. Results



(a) $\Delta t_{error} = 10$ $t_{threshold} = 75$

(b) $\Delta t_{error} = 15$ $t_{threshold} = 75$

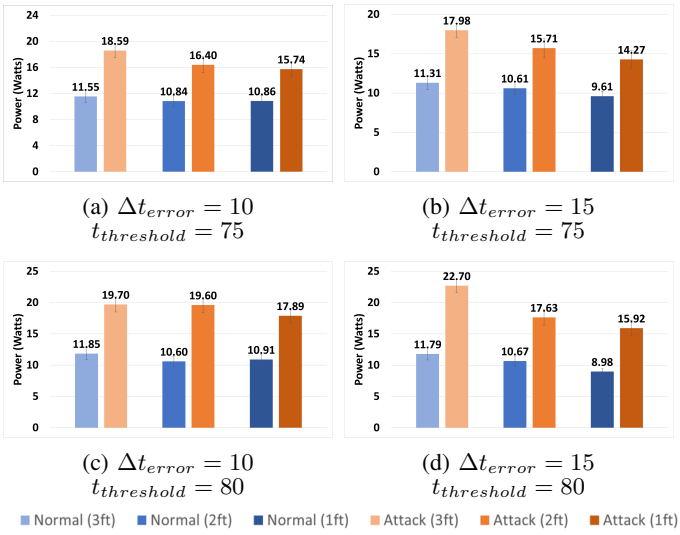
(c) $\Delta t_{error} = 10$ $t_{threshold} = 80$

(d) $\Delta t_{error} = 15$ $t_{threshold} = 80$

Figure 2: Cumulative Power Waste over Time graphs.

A. Effect of Δt_{error}, $t_{threshold}$, Distance and Time on Average Power

Fig. 3a show Average Power Graph for the $\Delta t_{error} = 10$ / $t_{threshold} = 75$ condition. The average power reading



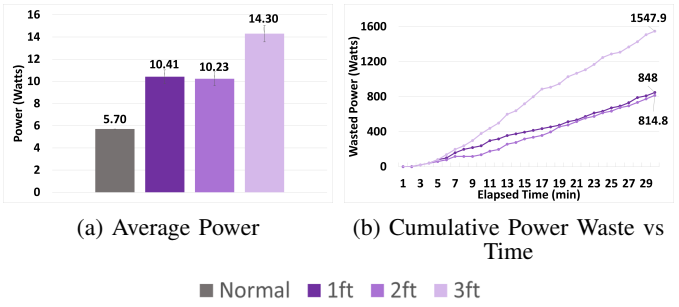
(a) $\Delta t_{error} = 10$ $t_{threshold} = 75$

(b) $\Delta t_{error} = 15$ $t_{threshold} = 75$

(c) $\Delta t_{error} = 10$ $t_{threshold} = 80$

(d) $\Delta t_{error} = 15$ $t_{threshold} = 80$

Figure 3: Average Power Graphs.



(a) Average Power

(b) Cumulative Power Waste vs Time

Figure 4: $\Delta t_{error} = 10$, $t_{threshold} = 80$, 30-min test graphs

was 11.55W for the *normal* condition, and 18.59W for the *attack* condition. The average power reading for the *normal* condition, and 16.40W for the *attack* condition. The average power reading was 10.86W for the *normal* condition, and 15.74W for the *attack* condition. Figures 3b ,3c, 3d and 4a can be interpreted the same way.

B. Effect of Δt_{error}, $t_{threshold}$, Distance and Time on Power Waste

Fig. 2a show the associated Cumulative Power Waste vs. Time graph for the $\Delta t_{error} = 10$ / $t_{threshold} = 75$ condition. The average power reading was 11.55W for the *normal* condition, and 18.59W for the *attack* condition. The average power reading for the *normal* condition, and 16.40W for the *attack* condition. The average power reading was 10.86W for the *normal* condition, and 15.74W for the *attack* condition. Figures 2b ,2c, 2d and 4b can be interpreted the same way with similar conclusions.

IV. Conclusions

Throughout this paper we look at the potential harm that a Trojan can do to data centers and systems of all types when it comes to sensor misreadings of temperatures. These false readings could end up meaning that there will be much more power consumption to cool the CPU down, reduce efficiency, and will end up being a very costly process. In the sessions provided in the graphs we validate that there is significant excessive power use with a Trojan giving sensors inaccurate readings compared to tests that do not have a Trojan and have normal correct sensor readings. The impact of these results shows us that within 10 minutes with temperature at 80 degrees and added error of 10 degrees you could end up losing up to around an extra 60% of power consumption and a cumulative 80% increase in power consumption. The difference for 10 minutes in cost would equate to around an extra 2.6$ per day, 936 dollars per year, and for 30 minute tests this could equate up to around 7.16$ per day, and 2,579 dollars per year accordingly for a simple multicore chip like Raspberry Pi.

References

[1] https://energyinnovation.org/2020/03/17/how-much-energy-do-data-centers-really-use/.

[2] S. Greenberg, E. Mills, B. Tschudi, L. Berkeley, N. Laboratory, P. Rumsey, and R. Engineers, "Best practices for data centers: Lessons learned from benchmarking 22 data centers," in *Proceedings of the ACEEE Summer Study on Energy Efficiency in Buildings in Asilomar, CA. ACEEE*, 2006, pp. 76–87.

[3] https://eta.lbl.gov/publications/united-states-data-center-energy.

[4] C. Patel, C. Bash, R. Sharma, M. Beitelmal, and R. Friedrich, "Smart cooling of data centers," 01 2003.

[5] C. Bash, C. Patel, and R. Sharma, "Dynamic thermal management of air cooled data centers," in *Thermal and Thermomechanical Proceedings 10th Intersociety Conference on Phenomena in Electronics Systems, 2006. ITHERM 2006.*, 2006, pp. 8 pp.–452.

[6] R. Zhou, Z. Wang, C. E. Bash, A. McReynolds, C. Hoover, R. Shih, N. Kumari, and R. K. Sharma, "A holistic and optimal approach for data center cooling management," in *Proceedings of the 2011 American Control Conference*, 2011, pp. 1346–1351.

[7] F. J. Mesa-Martinez, E. K. Ardestani, and J. Renau, "Characterizing processor thermal behavior," *SIGARCH Comput. Archit. News*, vol. 38, no. 1, p. 193â204, mar 2010. [Online]. Available: https://doi.org/10.1145/1735970.1736043

[8] J. Kong, S. W. Chung, and K. Skadron, "Recent thermal management techniques for microprocessors," *ACM Comput. Surv.*, vol. 44, no. 3, jun 2012. [Online]. Available: https://doi.org/10.1145/2187671.2187675

[9] J. Zhang, F. Yuan, and Q. Xu, "Detrust: Defeating hardware trust verification with stealthy implicitly-triggered hardware trojans," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 153–166.

[10] A. Webber and A. Haj-Omar, "Calculating useful lifetimes of temperature sensors," *TI Application Report*, July 2018.