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

Michael Kausch, Andrew Ibrahim and Dr. Mostafa Abdelrehim

Department of Computer Science and Computer Engineering, California State University, Bakersfield

Introduction

Some of the world's cloud computing centers require ~100MW under normal operations [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 [2]. Data centers that use efficient cooling strategies can reduce total power consumption anywhere from 33% to 50% [3-5].

Dynamic Thermal Management techniques are used to maintain local cooling which relies heavily on CPU thermal sensors to properly report an accurate temperature [6]. When the embedded cooling power is not enough to overcome individual processor heat [5], the facility's centralized cooling power increases accordingly which increases energy cost.

Improper reporting of CPU temperature may happen due to either:

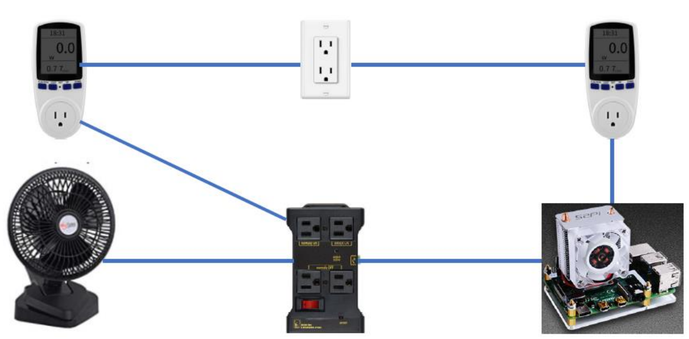
i. having unwanted modifications in the sensor circuit design in order to facilitate future security attacks (also known as Hardware Trojan) [7], or

ii. permanent or transient faults in the sensor or its accompanying circuitry [8].

We used a Raspberri Pi 4 to model a simple data center and a desk fan to model a simplified version of thermal management. The CPU was then subjected to a program that simulates the effects of a Hardware Trojan by causing T_{CPU} to be reported as T_{CPU} plus some error (T_{error}). We then measured the resultant power waste as a result of this security attack.

Our findings indicate that the resulting power causes a significant impact even at in our simplistic model.

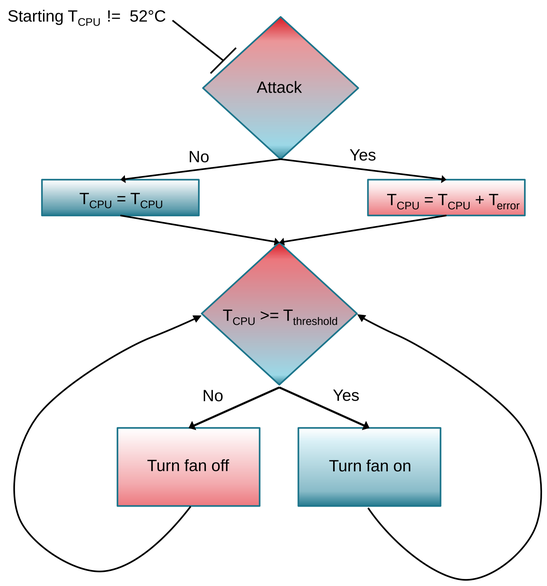
Methods: Setup



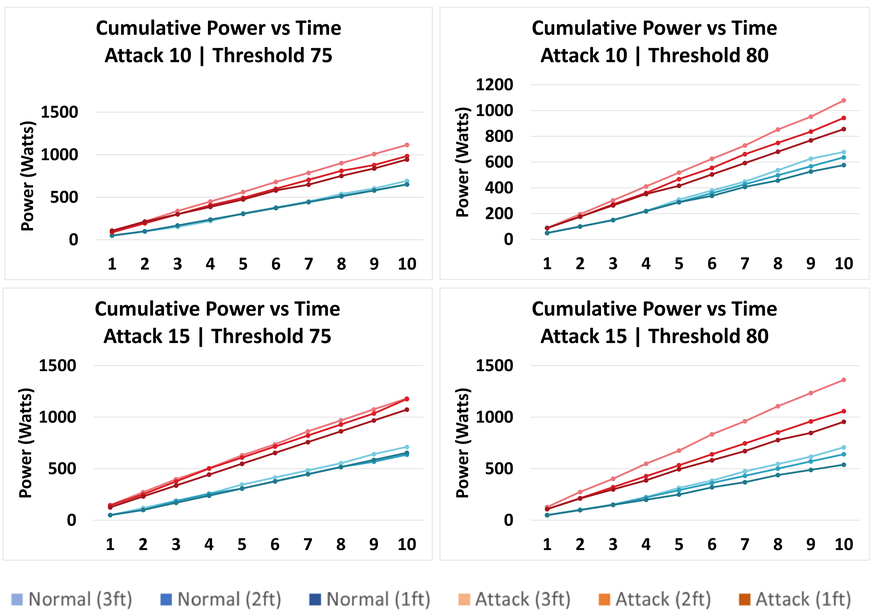
Independent Variables

- $T_{threshold}$ (75°C or 80°C)
  - Typical temps to begin cooling strategies
- T_{error} (10 °C or 15°C)
  - Hypothetical error added to T_{CPU} readings
- fan distance (1, 2 or 3 feet)
  - Simple way to model progressively less effective cooling strategies

Methods: Controlling Program



Results



References

[1] https://energyinnovation.org/2020/03/17/how-much-energy-do-datacenters-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.

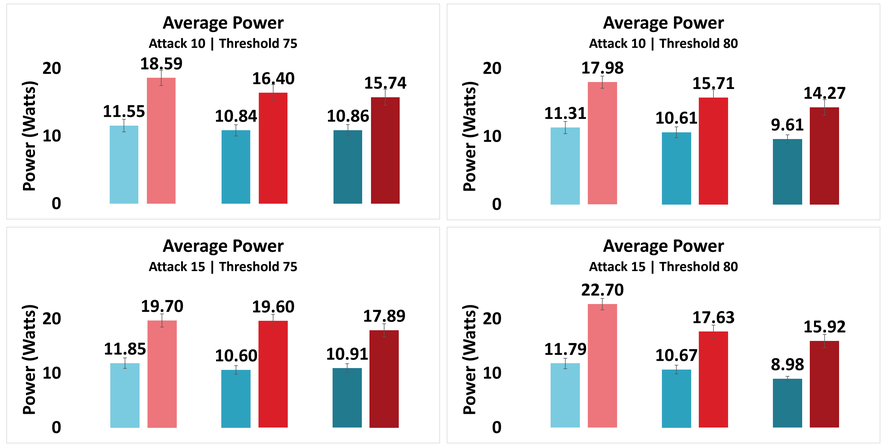
[5] C. Bash, C. Patel, and R. Sharma, "Dynamic thermal management of air cooled data centers," in *Thermal and Thermomechanical Proceedings 10th Intersociety Conference on Phenomena in Electronics Systems, 2006. ITHERM 2006.*, 2006, pp. 8 pp.–452.

[6] 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

[7] 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.

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

Results (continued)



Parameters			Total Power (W)		Power	% Increase in	*Cost in US Dollars ($) for:		
Δt_{error}	$\Delta t_{threshold}$	Dist (ft)	Normal	Attack	Waste	Power	1 hour	1 day	1 year
10	75	3	692.8	1115.6	422.8	61.03%	0.735672	17.656128	6444.49
10	75	2	650.6	984.1	333.5	51.26%	0.58029	13.92696	5083.34
10	75	1	651.3	944.3	293.0	44.99%	0.50982	12.23568	4466.02
10	80	3	678.5	1078.9	400.4	59.01%	0.696696	16.720704	6103.06
10	80	2	636.8	942.8	306.0	48.05%	0.53244	12.77856	4664.17
10	80	1	576.5	856.3	279.8	48.53%	0.486852	11.684448	4264.82
15	75	3	710.8	1181.7	470.9	66.25%	0.819366	19.664784	7177.65
15	75	2	636.2	1176	539.8	84.85%	0.939252	22.542048	8227.85
15	75	1	654.3	1073.3	419.0	64.04%	0.72906	17.49744	6386.57
15	80	3	707.3	1361.8	654.5	92.53%	1.13883	27.33192	9976.15
15	80	2	640.4	1057.9	417.5	65.19%	0.72645	17.4348	6363.70
15	80	1	538.7	955.1	416.4	77.30%	0.724536	17.388864	6346.94

* - Cost assumes an average cost of $0.29/kWh in California with continuous/uninterrupted use

Conclusions

These experiments validates the potential harm that a Trojan can do to data centers and systems of all types when it comes to improper thermal sensor readings. 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 very costly compared to that have normal/correct sensor readings.

The impact of these results shows us that if we chose a reasonable threshold cooling temperature of 80°C to begin our cooling strategy and if the reported error was off by +10°C, this would result in an extra ~60% power consumption at the furthest distance. Assuming an average cost of $0.29 / kWh which is the average in Bakersfield, California, this would result in an increased operational cost by nearly $6,100 for a simple multicore chip like Raspberry Pi.

In the most extreme scenario, at the least efficient distance of 3ft where the threshold temperature was again 80°C but the error was set to 15°C, our measurements showed an increase in power consumption of 92% which would result in a $9,900 increase in cost!

While these results pertain to our specific cooling strategy on one processor, its easy to extrapolate and see that this vulnerability could have significant financial impacts on large scale data centers.

Acknowledgements

This work is supported by the CSUB Summer Undergraduate Research Experience program.