ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 11, November 2022

Thermal Attack In Linux System

[1] Naveen J, [2] Mohit Raj, [3] Navya Bhatt, [4] Rakshitha M, [5] Poornima Arya, [6] Dr. Anusha Preetham

[1][2][3][4] [5] Students, DSATM, Bengaluru, India
[6] Faculty, DSATM, Bengaluru, India
Email: [1] naveenjk8417@gmail.com,[2] 1726mohitraj@gmail.com, [3] bhattnavya3110@gmail.com,
[4] rakshitham0904@gmail.com, [5] aryapoornima123@gmail.com

***Abstract*— Many operating systems now a days make use of thermal sensors for monitoring the CPU temperature. The monitoring of CPU temperature mainly includes measuring the frequency, energy consumption temperature of the CPU. Some unprivileged users can make use of this thermal sensor to gain access to some secret information. The unprivileged users used to execute programs in order to generate heat within the CPU in order to generate the covert channel in which leakage of information may take place.**

I. INTRODUCTION

In this paper we mainly deal with the thermal side channel attack of thermal sensors in Intel CPU. On the basis of some of the research on Running Average Power Limit (RAPL) in Intel CPU can be a reliable leakage source. For this particular reason the recent version of Linux does not use RAPL. Particularly in this paper we show that there is still a vulnerable interface for leakage of information due to thermal attack in Linux systems. We also explain the properties of thermal sensors and distinguish the cache hit and the access of the physical memory by monitoring the thermal sensors. This paper highlights the concept of Thermal Bleed in Linux systems. Thermal Bleed is used to break the (KASLR) Kernel Address Space Layout Randomization. The temperature will increase when accessed a valid address which is called dtLB hit. The temperature will decrease when accessed invalid address which is called dtLB miss. The sufficiently reliable channel will be formed due to the differences between the thermal miss and thermal hit. This will also cause randomization and it took around 9min in order to randomize KASLR with a complete accuracy. The Thermal Bleed is the first software based thermal side channel attack that it does not need any timings to deliver the attack. hwon is an interface which is used to monitor the hardware. This is used to fetch the data from CPU, motherboard and graphic processing unit. The Intel CPU in Linux only support hwon and it is not supported by other operating system such as window, mac. Therefore, we can see thermal bleed only in Linux system

II. BASES OF THE THERMAL SIDE CHANNEL ATTACK

A. THERMAL ANALYSIS

In this we mainly deal with the analysis of thermal side channel attack. Firstly, we look into the concept such as Law of conservation of energy which states that “Energy can neither be created nor destroyed but can be converted from one form to another” and the ohm’s law which states that “The amount of electric current flowing through the conductor is directly proportional to the potential difference between two end of the conductor”. With the help of these two law we came to the conclusion that heat can be expressed as the product of power consumption and voltage. H=P.t[J] This shows us that heat is directly linked with power. Thermal side channel analysis used to affect the data by prefetching security sensitive data such as secret keys

B. TRANSLATION OF ADDRESS

Each processor will have separate address in order to prevent overlapping of another processor. Address translation is nothing but manipulation of IP address over the internet. The system is more often referred to as Network Address Translation. When we talk about the address, they are basically two types which will consist of virtual page number and the page offset. These addresses are mainly controlled by the memory management unit (MMU). In a multi-level page walk it usually considers the page which will be translated into physical frame number. Thus, the page number can be obtained from the multi-level page walk. By obtaining page number will help us to access the physical address. These are done in the Address Translation Process.

C. RANDOMIZATION

The physical address causes the corruption of the Memory layout of the system. These attacks mainly deal with timing differences of the loaded and unloaded pages. Thus, we can say that this good strategy to attack the operating system. KASLR is vulnerable to like this type of the attack In Linux system has 9 bits of entropy and this can be guessed through 512 times of guessing in KASLR.

III. REASONS FOR THE ATTACK

In these we are going to the various reason which will cause this attack by conducting certain type of experiment in the Intel CPU. The experiment are as follows:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 11, November 2022

A. EXPLANATION OF THE EXPERIMENT

In this we are experiment we are considering the Intel CPU. We are going to execute various load program which will causes the cache hit or accessing of the address of the physical memory. For measuring the heat of the CPU while running the program we generally make the complete use of the collection application. The heat generated in the core will be then isolated. These are the aspects which will come under the experimental setup.

B. ACCESSING THE MEMORY

In this we are going to see how we are going to distinguish the cache access with the physical memory access. Since we know that the heat difference is the major need to describe the thermal side channel attack and hence this difference will become necessary in determining the heat. The heat will be generated outside the package so that the measurement will become physical. With the help of the thermal we are going to see where actually load is affected either by the cache or physical memory. This we are able to identify by measuring the temperature under various settings, physical memory access and the cache hit in by executing or without executing the load program.

C. TRANSLATION OF ADDRESS

In this we are showing that the thermal sensors are capable of differing the address .By measuring the TLB hit and misses and calculating the temperature. Then we are going to measure the temperature difference of these two hit. When the temperature hit is twice as higher than the temperature difference we are able to find out reliable channels. This process basically used to fetch the data from the cache to the memory needs which can basically be termed as Address Translation. Due to this very reason we are able to increase the attack surface of the thermal bleed attack in Linux System

IV. ANALYSIS OF THERMAL ATTACK

A thermal attack usually takes place in two phases they are

A. COLLECTION OF DATA

B. SIMPLE THERMAL ANALYSIS (STA)

A. COLLECTION OF DATA

In this the collector used to collect the data with the of hwon interface. For this he will make use of the collecting application as we had discussed earlier. Then we used to calculate the dtlb hits and misses with help of this data.This will mainly help in the randomization of the address and we can easily get the information.

B. SIMPLE THERMAL ANALYSIS (STA)

We know that the heat will be collected by the thermal sensors in order to distinguish the temperature we need the concept of thermal analysis. In this analysis we are mainly going to obtain the address of the kernel text. _entry_text_start is the symbol to switch page table and there is also startup_64 where there will be a loss of data. By subtracting the these two values we will obtain the base address. This was experimented with help of i-9-10900 CPU.

V. EVALUATION BASED ON VARIOUS FACTORS

A. NOISELESS KASLR BREAKING

Basically, thermal bleed is used to break KASLR from an unprivileged user. Now let us assume an situation of an ideal attack in which the temperature measurement during the attack is not altered by the noise. Usually during the first phase of the attack we will measure the core temperature. To acquire the temperature traces, we utilize our synchronization approach. After collection of the traces, we usually analyze to measure the temperature. There will be a variation between the heat capacity with respect to the resistance mainly due to the difference in architecture and number of frequencies which may affect the thermal bleed performance. Therefore, there will be the rerandomization of the KALSR with various model of CPU with

Certain limitation for capacity of heat and their resistance which may lead to thermal bleed.

B. LOCAL NOISE FROM A DIFFET

(Simultaneous Multithreading) could also be causing the noise. As a result, we use this scenario to assess the resilience of Thermal Bleed against SMT noise

CPU	# of traces (T_n)	Accuracy	Time	ThermalBleed
Core i7-7200U	300	40%	6 min	✓
	500	88%	9 min	
Core i7-10510U	300	37%	6 min	✓
	500	76%	9 min	
Core i7-6700K	300	63%	6 min	✓
	500	96%	9 min	
Core i5-7400	300	63%	6 min	✓
	500	99%	9 min	
Core i7-8700	300	67%	6 min	✓
	500	90%	9 min	
Core i5-9600K	300	62%	6 min	✓
	500	93%	9 min	
Core i7-10700	300	60%	6 min	✓
	500	95%	9 min	
Core i9-10900	300	65%	6 min	✓
	500	100%	9 min	
Xeon E3-1279 v6	300	65%	6 min	✓
	500	100%	9 min	
Xeon Silver 4210	300	63%	6 min	✓
	500	91%	9 min	

C. P-STATE CHANGES

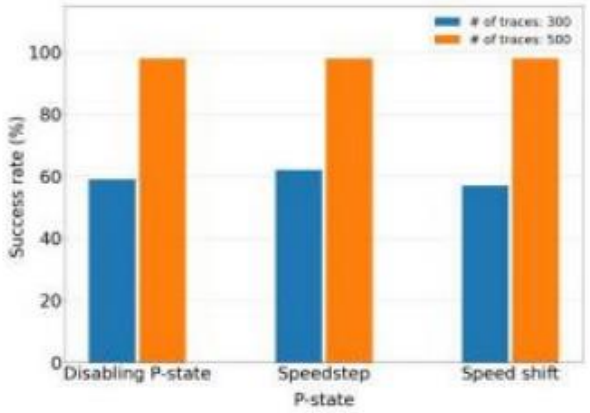
Basically, Speed Step and Speed Shift are the two models which are offered by intel. Even sometimes they used to share the similar destiny of effective management of power and they usually work in a very different manner. The OS chooses the voltage and frequency for Speed Step based on the current workload. However, for Speed Shift, these elements are

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 11, November 2022

managed by the Power Control Unit (PCU). P-state modifies power management behavior based on the workload of the system. As a result, changes in power consumption and CPU temperature occur.



P STATE CHANGE

VI. PROPERTIES OF THERMAL SENSOR

Thermal bleed sensors are located outside the CPU and therefore the temperature measurement is done outside. Due to this very reason, we can tell the difference between cache access which occurs inside the CPU and the physical memory access which occurs outside the CPU. In the figure 2 and 3 shows that the physical core shows the greater temperature than the baseline. Therefore, we are able to say that there will be minor impact on the physical memory access in the basis of temperature. As a result, we do research to determine what causes the CPU temperature to rise. We mainly determined that the quantity of electric current and the voltage is basically the cause for the core temperature with respect to the CPU. We came to this conclusion with help of Joules law of heating and the ohms law. One of the parameters that can affect the core temperature is the Hamming weight of the operand value in an instruction. It comes from the fact that the Hamming weight is proportional to the amount of voltage required for the CPU to execute instructions. The sum of all the resistances in the CPU that are involved in executing the instructions is usually constant. As a result, the amount of voltage applied to the CPU was proportionate to the quantity of electric current, according to Ohm's law. . As a result, the Hamming weight of the operand value has an effect on the CPU's heat generation. Second, we hypothesized that the IPC and core temperature are closely connected. In fact, earlier research has found that there is a strong link between power usage and IPC . As a result, we test our hypothesis by looking at the association between core temperature and IPC.

TABLE 4 shows the average core temperature and IPC for instructions with different operands.

Operand	imul r64		Operand	shl r64, imm8	
(r64)	Temp.	IPC	(imm8)	Temp.	IPC
Baseline	27.046 °C	-	Baseline	27.885 °C	-
0x00	30.855 °C	0.67	0x00	31.759 °C	1.0
0xff	30.951 °C	0.67	0x3f	31.855 °C	1.0
0xffff	31.048 °C	0.67	0x7f	31.903 °C	1.0
0xffffff	31.336 °C	0.67	0xbf	31.951 °C	1.0
0xffffffff	31.567 °C	0.67	0xff	31.962 °C	1.0

We turned off Intel Turbo Boost and set the CPU frequency as a base frequency to reduce noise during the experiment. Due to the heat in the CPU core can also destruct the trustworthy experiment. As a result, we run our apps on distinct cores: the target application runs on core 0, while the collecting application runs on the core that is farthest from core 0. Because of the thermal capacity and resistance, residual heat may obstruct temperature measurement. As a result, we begin with the instruction with the highest IPC and work our way down to the next instruction when the current core temperature matches the baseline temperature. For two instructions, "imul r64" and "shl r64, imm8," we first measured the core temperature and IPC. The values of those two operands range from 0 00 to 0xffffff on an i7-8700 CPU, Table 4 shows the measurements of core temperature and IPC when issuing the instructions (i.e., imul and shl). The value of IPC is consistent over the operand values because we deactivated Intel Turbo Boost and fixed the frequency at 3.2 GHz (i.e., basic processor frequency). The amount of voltage and current on the CPU is affected by the operand value, whereas an arithmetic instruction has a constant delay regardless of its operand value . As a result, the temperature rises in proportion to the Hamming weight of the operand value . In "imul 0 00" and "shl r64, 0 00" instructions on an i7-8700 CPU result in temperatures of 30.855°C and 31.759°C, respectively. The CPUs were given the bare minimum of voltage and current in this situation. The instructions "imul 0xffffffff".

Inst.	i7-10510U		i7-8700	
	Temp.	IPC	Temp.	IPC
baseline	38.717 °C	-	30.000 °C	-
DRAM access	43.047 °C	0.01	31.144 °C	0.01
dTLB miss	43.857 °C	0.05	31.288 °C	0.05
aesenc xmm1, xmm0	44.474 °C	0.50	31.663 °C	0.50
imul rax, rbx	44.759 °C	0.67	32.567 °C	0.67
inc rax	45.952 °C	2.0	34.673 °C	2.0
xor rax, rbx	46.472 °C	2.0	34.134 °C	2.0
cache hit	46.762 °C	2.0	34.989 °C	2.0
dTLB hit	47.000 °C	2.99	35.240 °C	2.99

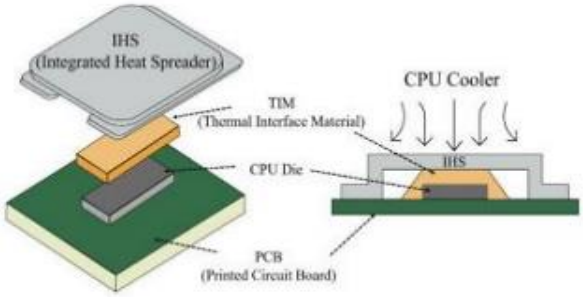
TABLE 5 shows the average core temperature and IPC for different instructions.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 11, November 2022

VII. STRUCTURE OF CPU PACKAGE



It's understandable that thermal sensors aren't designed to record temperatures mainly in the outer section of the CPU chip, and that compute-intensive programmes may generate higher temperatures than others. As a result, prior studies investigated the reported behavior without thoroughly examining the thermal sensor. Instead of considering a precise and effective thermal side-channel attack, the current research was limited to a simple. thermal hidden channel. We investigated Intel thermal sensors in depth in order to encourage more study into software-based thermal side-channel attacks. With the following questions, we look into several thermal properties in particular. The location of the Intel digital heat sensors in the CPU packaging is investigated. Figure 9 depicts the CPU package's internal construction and a longitudinal segment. A thermal interface material (TIM) is a composite material that facilitates thermal coupling by transferring heat between interfaces. An integrated heat spreader (IHS) is a thin metal shell with excellent thermal conductivity that shields the CPU die from external threats and serves as a heat transfer interface between the processor and the heatsink (i.e., cooling device). From the heatsink to the IHS, TIM, and CPU die, the CPU cooler cools the CPU die. Intel digital heat sensors were installed in the CPU in this structure. The sensors were precisely installed in each core to measure the heat produced by the core. As a result, the Intel digital thermal sensors retrieve the data directly. the temperature inside the body, not the temperature outside the body the outcome (i.e., DRAM). In order for physical memory access to have an impact, the temperature of the core, as well as the heat created by the DRAM should raise the temperature of the air the hot air then causes a disturbance. the efficiency of the CPU cooling, which has an indirect impact on the Temperature of the CPU. As a result, a load from physical memory is performed. has a significantly reduced impact on the temperature of the core, as well as the heat created by the DRAM should raise the temperature of the air the hot air then causes a disturbance. the efficiency of the CPU cooling, which has an indirect impact on the Temperature of the CPU. As a result, a load from physical memory is performed. has a significantly reduced impact on the thermal sensors installed in the core rather than a cache memory load As a result, Intel Cache access is more sensitive to digital thermal sensors than it is to analogue thermal sensor access to physical memory.

VIII. CONCLUSION

In this paper we see through the thermal sensor attack and thermal properties of the thermal sensors. We have done analysis about the CPU temperature with the help of hwon interface and find out how we are going to extract the information with the help of the thermal interface .We believe that these properties can be useful to construct more stable thermal side channel attack. The vulnerability will cause much security issues and should be restricted only to the privileged system user to secure the system.

REFERENCES

[1] S. J. Murdoch, ‘‘Hot or not: Revealing hidden services by their clock skew,’’ in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2006, pp. 27–36.

[2] M. Alagappan, J. Rajendran, M. Doroslovački, and G. Venkataramani, ‘‘DFS covert channels on multi-core platforms,’’ in *Proc. IFIP/IEEE Int. Conf. Very Large Scale Integr. (VLSI-SoC)*, Oct. 2017, pp. 1–6.

[3] M. Lipp, A. Kogler, D. Oswald, M. Schwarz, C. Easdon, C. Canella, and

[4] D. Gruss, ‘‘PLATYPUS: Software-based power side-channel attacks on x86,’’ in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2021, pp. 355–371.

[5] Z. Zhang, S. Liang, F. Yao, and X. Gao, ‘‘Red alert for power leakage: Exploiting Intel RAPL-induced side channels,’’ in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, May 2021, pp. 162–175.

[6] Intel. (2020). *Running Average Power Limit Energy Reporting/CVE-2020-8694, CVE-2020-8695/INTEL-SA-00389*. [Online]. Available: https://software.intel.com/content/www/us/en/develop/articles/software-

[7] % security-guidance/advisory-guidance/running-average-power-limit-energy-reporti% ng.html

[8] D. Gruss, M. Lipp, M. Schwarz, R. Fellner, C. Maurice, and S. Mangard, ‘‘KASLR is dead: Long live KASLR,’’ in *Proc. Int. Symp. Eng. Secure Softw. Syst. (ESSoS)*, vol. 10379, 2017, pp. 161–176.

[9] Intel. (2019). *Deep Dive: Intel Analysis of Microarchitectural Data Sampling*. [Online]. Available: https://software.intel.com/content/www/us/en/develop/topics/software-se% curity-guidance.html

[10] R. J. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, and S. Capkun, ‘‘Thermal covert channels on multi-core platforms,’’ in *Proc. 24th USENIX Secur. Symp.*, 2015, pp. 865–880.