IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 1, January 2018

BUGS in Silicon

[1] Dr. Latika Kharb, [2] Permil Garg
[1] Associate Professor, [2] Student
Jagan Institute of Management Studies (JIMS), Delhi, India.

Abstract: - **In computing system, a processor refers to an electronic circuit which performs operations on some external data which is stored in usually memory or some other data stream like Hard-disk, Flash-drive, etc. The market leaders in manufacturing CPU's are Intel, AMD and ARM. MMX, SSE, SSE2, SSE3, SSE 4, SSE 4.1, SSE 4a, SSE4.2, SSE5, x86-64, AMD-V, Intel-VTx, AVX, AVX2, AVX-512, AES, SHA, FMA3, FMA4, F16C, XOP, 3D-NOW are the major instruction set present in today's CPU's. In this paper, we will discuss literature study on available processors and emphasized on Bugs in processors that are top marketers today.**

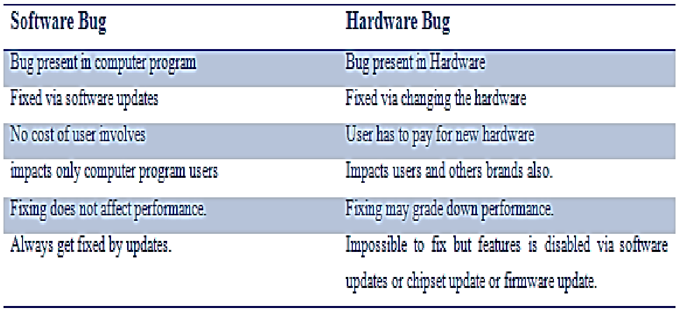
I. INTRODUCTION

In computing system, a processor refers to an electronic circuit which performs operations on some external data which is stored in usually memory or some other data stream like Hard-disk, Flash-drive, etc. There are various types of processors such as CPU - central processing unit, GPU - graphics processing unit, VPU - video processing unit, TPU - tensor processing unit, NPU - neural processing unit, PPU - physics processing unit, DSP - digital signal processor, etc. but the central processor (Central processing unit or CPU) is frequently referred as processor. An electronic circuit made up of logic gates which carry out the basic arithmetic, logical, control and input/output (I/O) operations on the data and those operations are specified by the instructions and that electronic circuit is known as a central processing unit (CPU). A CPU has mainly consist of arithmetic logic unit (ALU) that performs arithmetic and logic operations, registers that store data or result and provide operands to ALU and control unit that co-ordinate the fetching of data from various sources and execution of instructions. The single integrated electronic circuit (IC) is most common form of processors now days.

The market leaders in manufacturing CPU's are Intel, AMD and ARM. MMX, SSE, SSE2, SSE3, SSE 4, SSE 4.1, SSE 4a, SSE4.2, SSE5, x86-64, AMD-V, Intel-VTx, AVX, AVX2, AVX-512, AES, SHA, FMA3, FMA4, F16C, XOP, 3D-NOW are the major instruction set present in today's CPU's.

1.2. What is Bug?

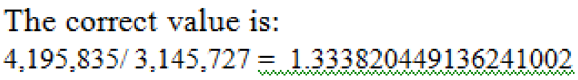
When a computer program produce an incorrect or unexpected results or behave in unintended ways due to a flaw, failure or any fault is refers to a BUG and when a bug is exploited to gain unauthorized access or privileges on a computer system are called a security bug. Any vulnerability in system which is exploited to bypass Authentication of user or other entities, to get authorization of access rights and privileges and to breach the data confidentiality is considered as security bug. The main causes of bugs are poor designing of system. Bugs are classified into two types namely, Software Bug and Hardware Bug.



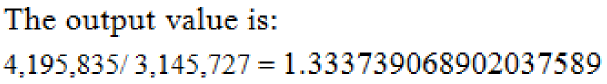
Software Bug	Hardware Bug
Bug present in computer program	Bug present in Hardware
Fixed via software updates	Fixed via changing the hardware
No cost of user involves	User has to pay for new hardware
impacts only computer program users	Impacts users and others brands also.
Fixing does not affect performance.	Fixing may grade down performance.
Always get fixed by updates.	Impossible to fix but features is disabled via software updates or chipset update or firmware update.

1.3. Examples of bugs

- The Pentium FDIV bug was a bug that affected the floating point unit (FPU) of the early Intel Pentium processors which is discovered in 1994 by Professor Thomas R. Nicely at Lynchburg College. Because of the bug, the processor could return incorrect binary floating point results when dividing a number.This problem occurs only on some models of the original Pentium processor. Example



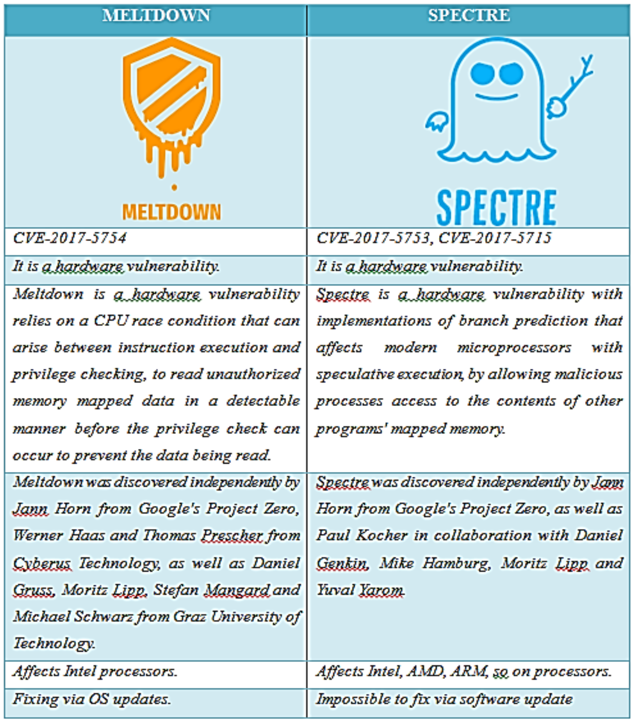
The correct value is:
4,195,835/ 3,145,727 = 1.333820449136241002



The output value is:
4,195,835/ 3,145,727 = 1.333739068902037589

As a result, the value returned by a flawed Pentium processor is incorrect at or beyond four digits.

- The Pentium F00F bug is a design flaw in the majority of Intel Pentium, Pentium MMX, and Pentium OverDrive processors (all in the P5 microarchitecture). Discovered in 1997, it can result in the processor ceasing to function until the computer is rebooted. The bug has been fixed through operating system updates.
- Google has just published details on two vulnerabilities named Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753, CVE-2017-5715) on 3 January, 2018.



MELTDOWN	SPECTRE
MELTDOWN	SPECTRE
CVE-2017-5754	*CVE-2017-5753, CVE-2017-5715*
It is a hardware vulnerability.	*It is a hardware vulnerability.*
Meltdown is a hardware vulnerability relies on a CPU race condition that can arise between instruction execution and privilege checking, to read unauthorized memory mapped data in a detectable manner before the privilege check can occur to prevent the data being read.	*Spectre is a hardware vulnerability with implementations of branch prediction that affects modern microprocessors with speculative execution, by allowing malicious processes access to the contents of other programs' mapped memory.*
Meltdown was discovered independently by Jann Horn from Google's Project Zero, Werner Haas and Thomas Prescher from Cyberus Technology, as well as Daniel Gruss, Moritz Lipp, Stefan Mangard and Michael Schwarz from Graz University of Technology.	*Spectre was discovered independently by Jann Horn from Google's Project Zero, as well as Paul Kocher in collaboration with Daniel Genkin, Mike Hamburg, Moritz Lipp and Yuval Yarom.*
Affects Intel processors.	*Affects Intel, AMD, ARM, so on processors.*
Fixing via OS updates.	*Impossible to fix via software update*

II. ANALYSIS ON BUGS

An attacker can exploit these microprocessor vulnerabilities to expose extremely sensitive data which resides in the protected kernel memory. That data includes passwords, cryptographic keys, personal photos, emails, or any other data on your PC.

As per Google believes "every Intel processor which implements out-of-order execution is potentially affected, which is effectively every processor since 1995 (except Intel Itanium and Intel Atom before 2013)" is affected by Meltdown and Meltdown only against Intel CPUs, but not ARM and AMD. Nonetheless, Intel has a market share of than 80% on desktops and more than 90% on the laptop and server markets, meaning that a large number of desktops, laptops, and servers are affected. Meltdown's impact on mobile devices is unknown, but patches are already available for Android.

2.1. Modes of Micro processor

In a system, a microprocessor has basically 2 modes, User-mode and kernel-mode. User mode prevents access to that code and data which is stored in kernel mode. While microprocessor in user mode, the kernel's code and data remains out of sight from the programs and it provides a security layer on highly sensitive data of an operating system. Operating systems always runs all programs in user mode to prevent reading or corruption of sensitive data. A running program does lots of works such as reading/writing data to a file or allocate some memory or open a network connect, etc. Whenever a running program carry out these kinds of jobs it has to temporarily hand control of the processor to the kernel and to give control, program makes a system call and the processor is switched from user mode to kernel mode and kernel perform the given task. When it is done the CPU is told to switch back to user mode and the program is resumes it remaining working in user mode.

2.2. Solutions for Bugs in different Modes

While in user mode, the kernel's code and data remains out of sight but present in the process's page tables due to exploit in microprocessors it allows normal user programs – from database applications to JavaScript in web browsers – to discern to some extent the layout or contents of protected kernel memory areas. To fix this problem, separation of the kernel's memory completely from user processes using what's called Kernel Page Table Isolation, or KPTI. These KPTI patches move the kernel into a completely separate address space, so it's not just invisible to a running process, it's not even there at all. This separation of kernel memory is relatively expensive in terms of time wise because the switching between two separate address spaces for every system call and for every interrupt from the hardware. The implementation of KPTI is going to reduce the performance of machines due to overhead, some researchers claiming that there is loss of 5%-35% in performance depending on usage. Operating System developers are released emergency updates to implement KPTI patches.

- Linux kernel released patch kernel 4.9.75 onward.
- Apple already released the patches of macOSsince 10.13.2 High Sierra.
- Microsoft released an emergency update to Windows 10, 8.1, and 7 SP1 as well as Windows Server.
- Google also released patches for Chromebooksin Chrome OS 63, which released on December 15.
- Red Hat released kernel updates to their Red Hat Enterprise Linux distributions version 6 and version 7.
- CentOS also already released their kernel updates to CentOS-6 and CentOS-7.

Right now, you should update your operating system, CPU firmware (if available), and web browser and other software.

By January 12, Intel expects to have released firmware updates for 90 percent of processors released in the past five years.

III. CONCLUSION

The available vulnerability compromises entire server networks, not just individuals but individual users cannot upgrade their hardware because they ignore this kind of vulnerabilities. Even most of businesses are also ignoring it. They think it is just a waste of money. But servers must have to upgrade their hardware it may lead to a huge amount to upgrade their complete server rigs to feel their customers safe. Cloud services are also affected by the security problems. This time, Intel may provide processors at lower price.

REFERENCES

1. https://en.wikipedia.org/wiki/Central_processing_unit

2. https: // en. wikipedia. Org /wiki /Meltdown _(security_ vulnerability)

3. https : // en. wikipedia. Org /wiki /Spectre_ (security_ vulnerability)

4. https://en.wikipedia.org/wiki/Security_bug

5. https://en.wikipedia.org/wiki/Pentium_F00F_bug

6. https: // www. theregister. co. uk /2018 /01 /02 /intel_ cpu_ design_ flaw/

7. https :// www. bleeping computer. Com /news /security /google- almost- all- cpus- since- 1995- vulnerable- to-meltdown- and- spectre- flaws/

8. https : //www. engadget. Com /2018 /01 /04 /intel-patching- exploitable- processors /