Assignment: 1  
 Advance Operating System  
 Section: A  
 ID: 14-27173-2

One of the most important attributes of Operating System is Memory Management. Memory Management usually works with the memory of user space initially. If other task tries to disturb that user space, Memory Management redirects those tasks to another place. Usually when Memory Management can’t find any free space it usually clears the garbage or unused space by suspending and then sends process. If it fails to do it, it shows, not enough or sufficient memory message. And for that some situation occurs like Meltdown or Spectre.

**Meltdown**:

What is Meltdown?

Meltdown is a hardware vulnerability that allows rogue(bad) process to read all the memory, even it is not authorized and which is unexpected. For Meltdown performance loss is occurred.

It is almost like emotional meltdown in our real life when sometimes we feel so emotionally overwhelmed by unpleasant feelings that are not expected and we can’t get control over it.

How Meltdown works?  
Security issue of an Operating system of a computer depends on the Memory Management. Here kernel address ranges are marked as non-accessible and are protected from user access.  
  
It usually breaks the most fundamental detachment between user and application and operating system. By using the vulnerable processor meltdown gets access to the memory, as also the secrets of programs and operating system.

Meltdown uses the side effects of out of order execution on the modern processors which is an essential performance feature of the processor. It reads the independent kernel-memory location including various protected data. The attack is operating system independent. While a system is under attack, Meltdown enables an opponent to the read memory of other process or virtual machine in cloud without any permission or privileges. KAISER defense mechanism is used to protect Meltdown.

Which Platform it attacks?

Usually it attacks depending on hardware vulnerability, most commonly it affects Intel x86 microprocessors, IBM POWER Processors and some ARM-based microprocessors, this includes all devices running at the moment but the most recent and patched versions of iOS, Linux and macOS.  
  
But dell computers are yet to be reported under this kind of vulnerabilities.

How it can be prevented?

Some preventions are recommended to prevent meltdown. Such as, promptly adopting software updates, avoiding unrecognized hyperlinks and websites, not downloading files or applications from unknown sources, following secure password protocols, using security software to help protect against malware, advanced threat prevention software or anti-virus.

**Spectre**:

What is Spectre?

Like Meltdown Spectre is a security vulnerability discovered by Yann Horne from Google’s project zero that affects modern microprocessors that performs branch prediction. This allows attackers to access user’s private information at the CPU level.  
There various versions of Spectre attacks. Such as Spectre- V1, SPectre- V2, Spectre NG

How Spectre works?  
Attacker normally sends request as an arbitrary set of information to processor and get back a results through a variable from the CPU cache memory which value is of no use to the CPU. By checking many conditions and executing data of input attacker gets access of the private data. After guessing value from the cache memory attacker gets useful data or information and uses time-based attack to get the value.  
So, Therefore attacker runs code with misleading input. This tricks CPU into reading a secret character that it stored in the CPU cache memory and lastly attacker uses time based attack to get value and get access.

Which Platform it attacks?

Chips from Intel, AMD and ARM are under risk of Spectre attack.

How it can be prevented?  
The entire computer industry is trying to solve the problem as quick as possible. But for prevention the operating system and web browser should be updated on regular basis. Some patches are also available for preventing the situation.

Source:   
1. https://meltdownattack.com/  
2. <https://meltdownattack.com/meltdown.pdf>  
3. <https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)>

4. <https://www.pcworld.com/article/3245606/security/intel-x86-cpu-kernel-bug-faq-how-it-affects-pc-mac.html>

5. <https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)>