Spectre y Meltdown

Manzanares Peña Jorge Luis

Salazar Domínguez Jesús Eduardo

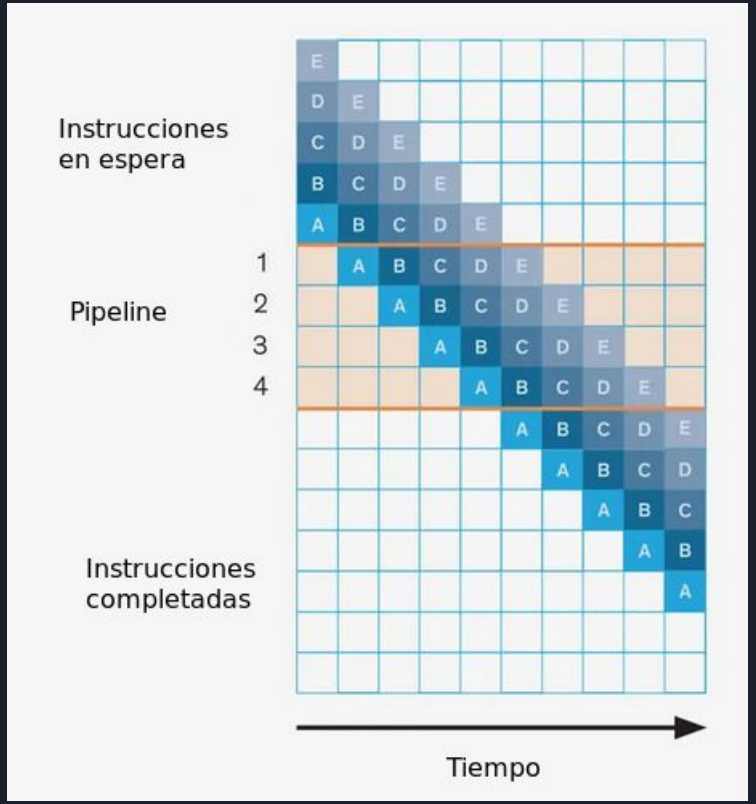
Introducción

- Los procesadores modernos tienen un funcionamiento muy diferente al que la mayoría de las personas cree.
- Son capaces de predecir el futuro, mejorando enormemente el rendimiento.
- La ejecución especulativa generó las condiciones propicias para la aparición de vulnerabilidades, como Spectre y Meltdown.

Segmentación de Instrucciones (Pipelining)

¿Qué es la segmentación de instrucciones?

- Técnica para implementar paralelismo a nivel de instrucciones.
- Define un *pipeline* conformado por diferentes etapas necesarias en la ejecución de una instrucción.
- Consigue mejoras significativas en el desempeño.



Nael Abu-Ghazaleh, Dmitry Ponomarev y Dmitry Evtyushkin. “How the spectre and meltdown hacks really worked”. En: IEEE Spectrum 56.3 (2019), págs. 42 - 49. D O I : 10.1109/MSPEC.2019.8651934

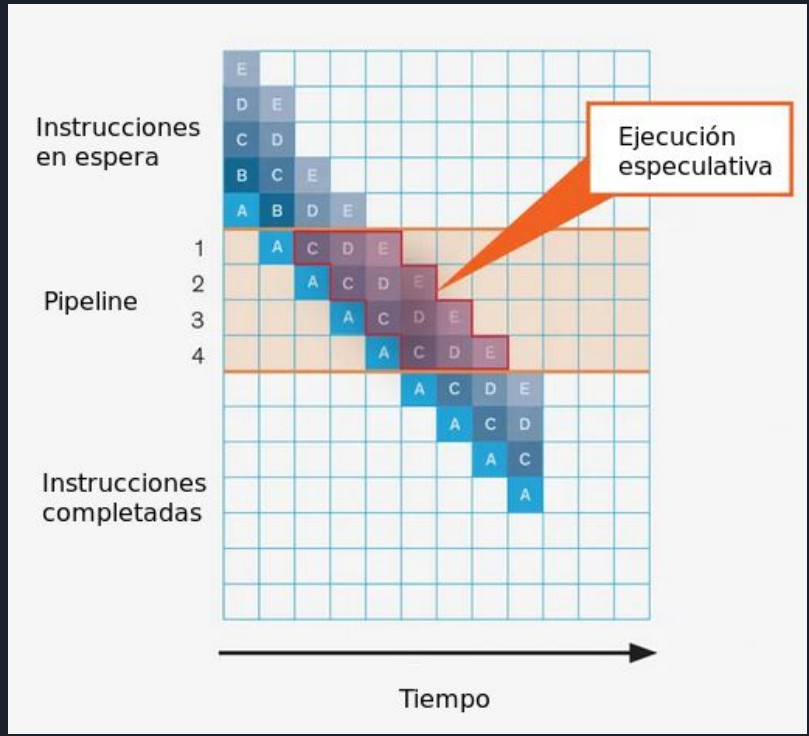
Ejecución especulativa

- La segmentación de instrucciones se enfrenta a un problema al encontrar saltos condicionales (*branching*).
- Al no saber qué camino tomará la ejecución, no puede determinar qué instrucción será la siguiente en el *pipeline*.
- Un programa suele ser 20% saltos condicionales.

Nael Abu-Ghazaleh, Dmitry Ponomarev y Dmitry Evtyushkin. “How the spectre and meltdown hacks really worked”. En: IEEE Spectrum 56.3 (2019), págs. 42 - 49. D O I : 10.1109/MSPEC.2019.8651934

Ejecución especulativa

- En la ejecución especulativa, un predictor de saltos adivina si el programa dará un salto condicional y a dónde.
- La instrucción siguiente especulada entra al *pipeline*.
- Si la especulación es incorrecta, los resultados generados deben ser descartados sin que el programa se entere.



Nael Abu-Ghazaleh, Dmitry Ponomarev y Dmitry Evtyushkin. "How the spectre and meltdown hacks really worked". En: IEEE Spectrum 56.3 (2019), págs. 42 - 49. D O I : 10.1109/MSPEC.2019.8651934

Ataques a la memoria caché

Memoria caché

- El caché es una memoria pequeña y rápida ubicada dentro del chip del procesador, cuyo objetivo es almacenar datos solicitados frecuentemente por el procesador durante la ejecución de un programa
- La memoria caché a menudo se vuelve un canal lateral de acceso.
- Una método de ataque a la memoria caché que ha sido utilizado para para comprometer algoritmo criptográficos, llamadas a funciones en servidores web, entradas de usuaria e información acerca de direcciones del kernel es Flush+Reload.

Meltdown

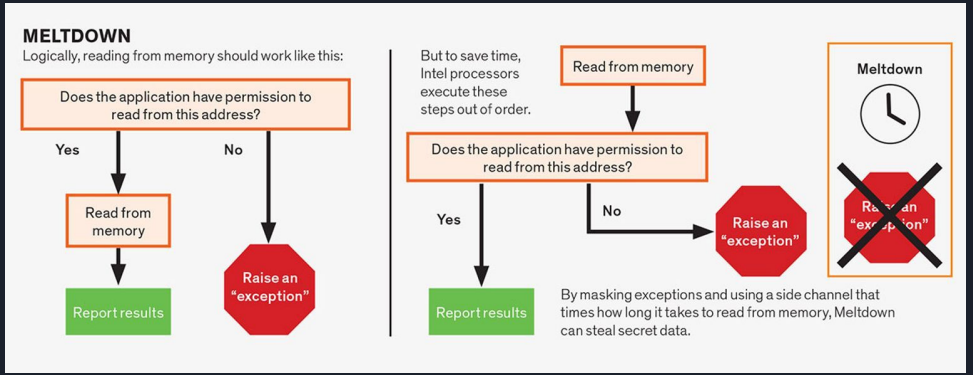
¿Qué es Meltdown?

- Vulnerabilidad presente en la mayoría de los procesadores modernos.
- Aprovecha la lectura especulativa de la memoria.
- Traspasa permisos y accede a datos confidenciales.

Funcionamiento

Meltdown accede a cualquier localidad mapeada en el espacio de memoria del proceso.

Utiliza un canal lateral para recuperar los datos leídos de forma especulativa.



Nael Abu-Ghazaleh, Dmitry Ponomarev y Dmitry Evtyushkin. "How the spectre and meltdown hacks really worked". En: IEEE Spectrum 56.3 (2019), págs. 42 - 49. D O I : 10.1109/MSPEC.2019.8651934

Etapas del ataque:

1. Lectura de una localidad de memoria.

2. Transmisión de los datos confidenciales.

3. Recepción de la información secreta.

Spectre

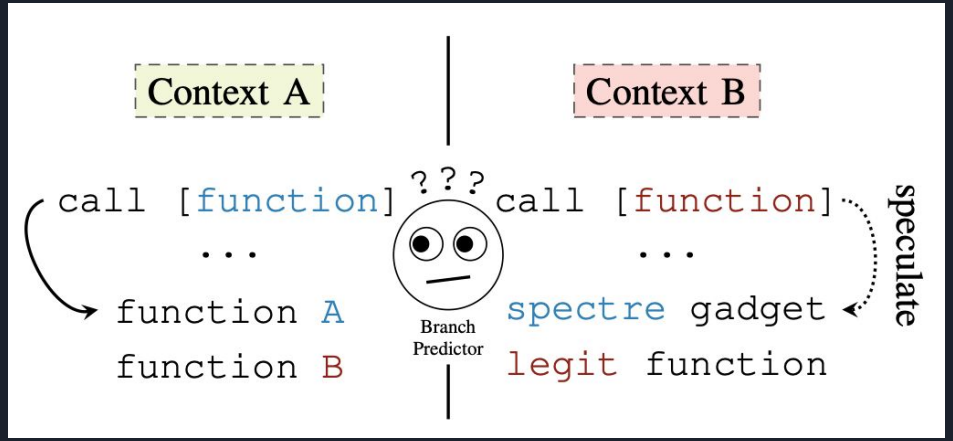
¿Qué es Spectre?

- Vulnerabilidad que se aprovecha de los sistemas predictores de saltos.
- Ejecuta acciones convenientes aprovechando la especulación.
- La víctima filtra los datos a los que tiene acceso.

Funcionamiento

Spectre engaña a una aplicación para acceder a cierta localidad dentro de su rango.

Utiliza un canal lateral para recuperar los datos leídos de forma especulativa.



Paul Kocher y col. “Spectre Attacks: Exploiting Speculative Execution”. En: 40th IEEE Symposium on Security and Privacy (S&P’19). 2019.

Etapas del ataque:

1. Entrenamiento malintencionado del predictor de saltos.

2. Ejecución especulativa errónea.

3. Recuperación de los datos confidenciales.

Spectre

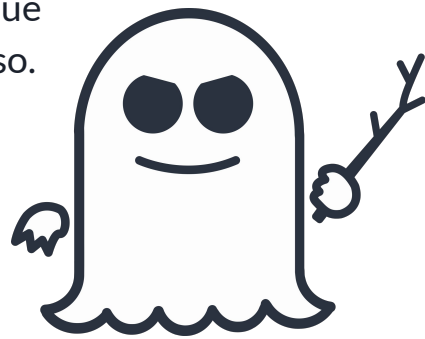
- Traspasa permisos y accede a datos restringidos, incluso a los del sistema operativo.

Puede filtrar una mayor cantidad de información.

Vs

Meltdown

- Engaña a otras aplicaciones para filtrar información a la que siempre ha tenido acceso.



Es más difícil de detectar y mitigar.

Consecuencias y Soluciones

Consecuencias

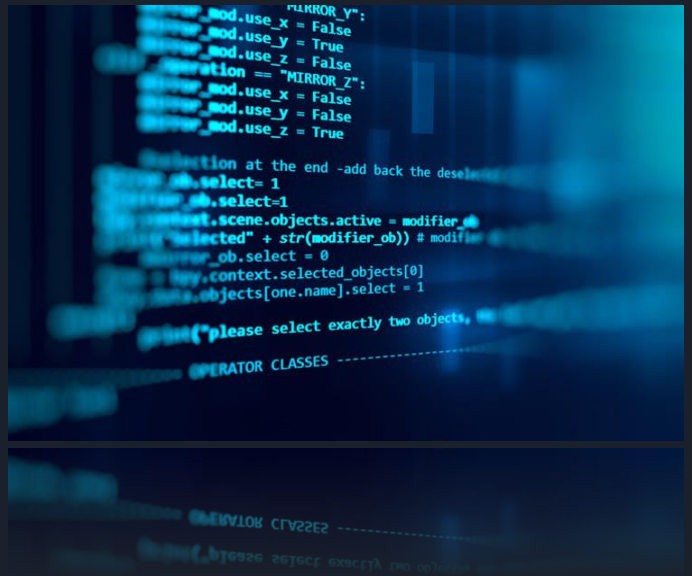
- Meltdown y Spectre representaron un duro golpe para la industria de la computación.
- Comprometieron prácticamente todos los sistemas fueran susceptibles a ellos, desde los celulares inteligentes, pasando por las computadoras personales y llegando hasta la nube
- Si bien el problema fue especialmente grave para los procesadores con arquitectura x86 de Intel, también se detectaron variantes de Spectre en ciertos procesadores AMD y ARM.
- No sé que tanto hayan sido explotadas (si acaso) estas vulnerabilidades para llevar a cabo ataques maliciosos

Soluciones a nivel software

- Tuvieron como objetivo limitar el alcance de los ataques.
- Eran respuestas incompletas a las vulnerabilidades.
- Redujeron el rendimiento de los sistemas considerablemente.

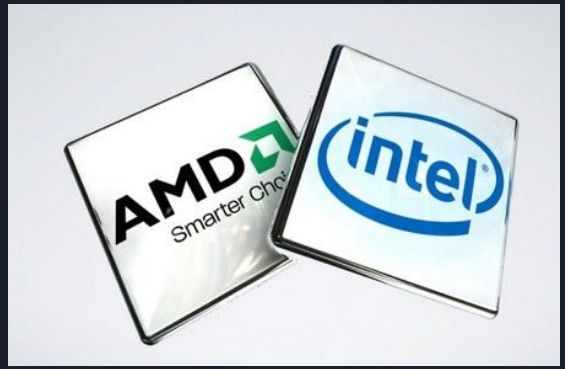
Ejemplo:

Aislamiento de tablas de páginas del núcleo (KPTI).



Soluciones a nivel hardware

Los fabricantes de procesadores (Intel, AMD) se vieron obligados a modificar su microcódigo y las operaciones a nivel ensamblador.



Procesadores en los que se confirmó la vulnerabilidad Meltdown:

Intel x86, ARM.

Procesadores en los que se confirmó la vulnerabilidad Spectre:

Intel x86, AMD, ARM.

Conclusiones

- Spectre y Meltdown representaron un desafío especialmente complejo por estar presentes en el hardware.
- Incluso las innovaciones tecnológicas más recientes presentan fallos y peligros.
- Spectre y Meltdown revolucionaron el mundo de la seguridad informática.

Bibliografía

- Nael Abu-Ghazaleh, Dmitry Ponomarev y Dmitry Evtyushkin. “How the spectre and meltdownhacks really worked”. En:IEEE Spectrum56.3 (2019), págs. 42-49.DOI:10.1109/MSPEC.2019.8651934.
- Benedict Herzog y col. “The Price of Meltdown and Spectre: Energy Overhead of Mitigations atOperating System Level”. En:Proceedings of the 14th European Workshop on Systems Security.EuroSec ’21. Online, United Kingdom: Association for Computing Machinery, 2021, págs. 8-14. ISBN: 9781450383370. DOI:10.1145/3447852.3458721. URL:https://doi.org/10.1145/3447852.3458721.
- Mark D. Hill y col. “On the Spectre and Meltdown Processor Security Vulnerabilities”. En:IEEEMicro39.2 (2019), págs. 9-19.DOI:10.1109/MM.2019.2897677.
- Paul Kocher y col. “Spectre Attacks: Exploiting Speculative Execution”. En:40th IEEE Symposiumon Security and Privacy (S&P’19). 2019.
- Moritz Lipp y col. “Meltdown: Reading Kernel Memory from User Space”. En:27th USENIX SecuritySymposium (USENIX Security 18). 2018.
- Andrew Prout y col. “Measuring the Impact of Spectre and Meltdown”. En:2018 IEEE HighPerformance extreme Computing Conference (HPEC). 2018, págs. 1-5.DOI:10.1109/HPEC.2018.8547554