INSTITUTO TECNOLÓGICO DE TIJUANA

SUBDIRECCIÓN ACADÉMICA

DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN

SEMESTRE
ENERO - JUNIO 2020

CARRERA:

INGENIERÍA EN SISTEMAS COMPUTACIONALES

MATERIA:
LENGUAJES DE INTERFAZ

Vulnerabilidades de ARM como MCU

Integrantes:
Reyna Cárdenas Marialaura
Salazar Hernández Leopoldo
Villarreal Felix Francisco Javier
Argaez Galindo Jesus Alexis
Garcia Rosas Ivan

NOMBRE DEL MAESTRO:
RENE SOLIS REYES

FECHA DE ENTREGA:
22/05/20

Introducción

La presente investigación se refiere al tema de las vulnerabilidades de ARM como MCU ya que en los últimos años ha sido un procesador muy usado dentro de los microcontroladores los cuales están facilitando la creación y administración de nuevas tecnologías en el mercado. Tomando en cuenta esto el hecho de que tenga vulnerabilidades es muy perjudicial para los productos más si ponen el peligro la información que se maneja de las tecnologías en las que se usa.

Para entender un poco más sobre las vulnerabilidades que tiene hemos realizado una investigación donde tocamos lo puntos más importantes como cuál es la debilidad de ARM, como afecta esto a las aplicaciones que se crean, así como las soluciones que se tienen para evitar que nuestros proyectos sean atacados.

Debilidades en el procesador

Los investigadores encontraron dos debilidades principales en los procesadores que podrían permitir a los atacantes leer información delicada que nunca debería abandonar la unidad de procesamiento central. Ambos problemas permiten a los atacantes leer información secreta que el procesador pone temporalmente a disposición fuera del chip.

Para que los procesos informáticos se ejecuten más rápido, un chip esencialmente adivinará qué información necesita la computadora para realizar su próxima función. Eso se llama ejecución especulativa. Como adivina, esa información sensible es momentáneamente más fácil de acceder.

Meltdown y Spectre como vulnerabilidades en ARM

Meltdown

La **vulnerabilidad Meltdown** surgió a raíz de que los CPU actuales pudieran ejecutar instrucciones fuera de orden. Se trata de una función muy cómoda que acelera el procesamiento de código, pero en algunos casos el CPU puede procesar código que es propenso a error, un código que no debería ejecutarse. Eso es, primero el CPU ejecuta el código y solo entonces se hace evidente que no se puede completar la acción, este tipo de situaciones suceden precisamente porque las instrucciones se han ejecutado fuera de orden.

Evidentemente, los resultados de estas operaciones no llegarán a ninguna parte, aunque dejarán rastros a nivel de microarquitectura, en la memoria caché del CPU, desde donde se podrían extraer. Como resultado, el caché se puede utilizar para recopilar datos que de otra forma serían inaccesibles: por ejemplo, una contraseña. Te contamos cómo funciona: un programa puede solicitar acceso a datos almacenados; el sistema, lógicamente, negará este acceso por falta de autorización. Pero, debido a la ejecución de operaciones fuera de orden, la contraseña acabará en el caché, desde donde es muy fácil de recopilar. En resumen, **Meltdown** podría tener lugar al intentar ejecutar una acción injustificada.

Spectre

La **vulnerabilidad Spectre** es similar a Meltdown, pero, aunque también está relacionada con la aceleración informática de la CPU, surge de la función de predicción de saltos de los CPU. Básicamente, un CPU es capaz de predecir estos saltos con cierto nivel de precisión, ya que la acción B suele ir precedida de la A. Por tanto, puede ejecutar la acción B antes de que se hayan esclarecido los resultados de A. Si la predicción ha sido correcta y la acción B sigue a la A, todo bien, y, si los resultados de A indican que el CPU debería de haber completado la acción con C, en lugar de B, el CPU abandonará el salto B y cambiará a otro en el que tenga que completar la acción C.

Como el predictor de saltos es inteligente, la mayoría de las veces recuerda el patrón de la acción, por lo que mejora el rendimiento del CPU (si B suele seguir a A, el CPU dará por hecho que en determinada situación tendrá que hacer B después de A). Pero se puede equivocar (a veces llega C en vez de B, aunque el predictor de saltos recuerda perfectamente que normalmente A va seguida de B).

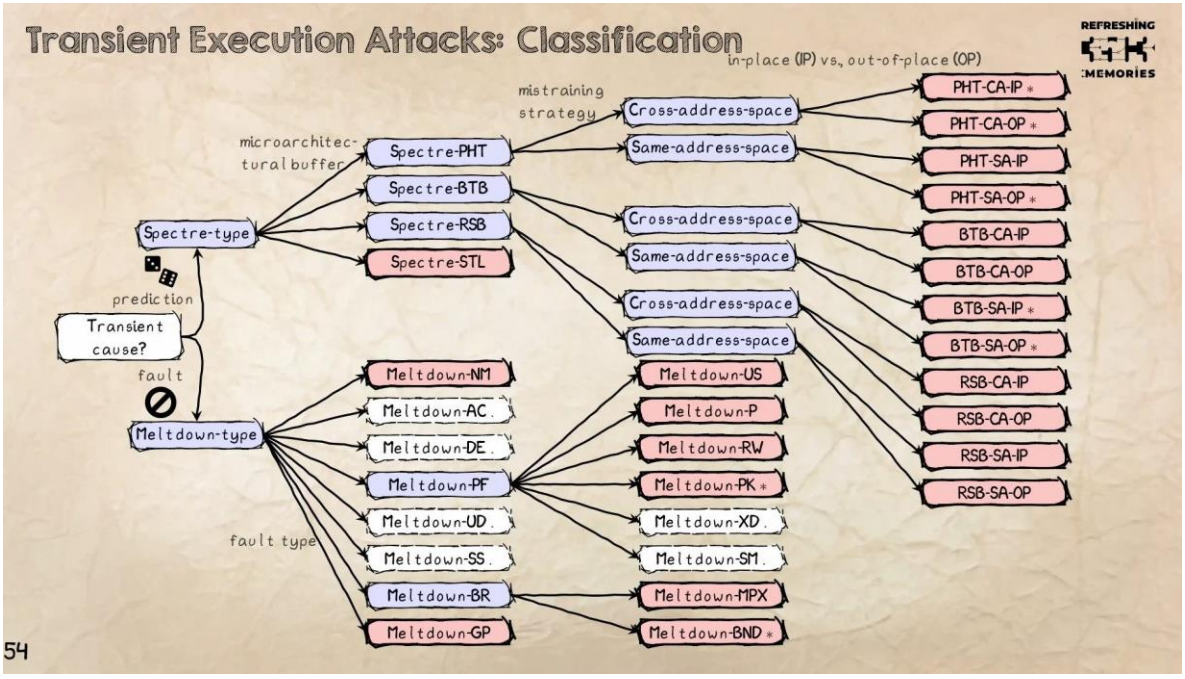
Si acostumbras al sistema a que cierto salto es el correcto y siempre se ejecuta y luego cambias un parámetro para que se equivoque, el CPU lo ejecutará primero y luego lo revocará, después de descubrir que debería de haber ejecutado otro. Pero, al igual que con Meltdown, el resultado de la acción puede permanecer, por ejemplo, en el caché, desde donde se podría volver a extraer.

Spectre 1 permite que una CPU sea engañada para cargar datos en un programa desde una dirección virtual de memoria ajena a los datos controlados por ese programa. Lo que hace, básicamente, es saltarse la verificación que hace que un programa no pueda acceder a ciertos datos por seguridad.

Spectre v2, una vulnerabilidad que consiste en engañar al sistema de predicción del procesador para que cargue datos externos en el BTB (Branch Target Buffer) seleccionados por el atacante. De esta manera se pueden leer datos directamente de los procesos que lo ejecuten, por ejemplo, contraseñas. Además, Spectre V2 permite que se pueda acceder a los datos de otros procesos ejecutados en el mismo hilo del procesador ya que el BTB (Branch Target Buffer) está compartido entre todos ellos.

Las consecuencias son casi las mismas: Spectre abre una trampilla para el **acceso no autorizado de datos**. Este acceso podría tener lugar solo en el caso de que la predicción de saltos saliera mal y, según la teoría de la probabilidad, pasaré tarde o temprano.

Ahora, si bien en primera instancia algunos de los importantes proveedores como ARM no son vulnerables a dichos fallos, más tarde fueron identificados nuevas variantes de estos mismo, aumentando el numero de estos de 2 a 27 vulnerabilidades. Entonces con el descubrimiento de estas variaciones, los que no podía afectar a ARM, lo logro, pero esto no es del todo oscuro, muchas de estas nuevas variaciones son incapaces de ser ejecutadas en ARM y otros proveedores, con lo cual, la tarea de darle solución o prevención a este tipo se fallas se reduce.



Con el objetivo de poner fin a estas vulnerabilidades, en enero del 2018, las empresas comenzaron a lanzar parches para microcódigos de CPU, sistemas operativos y programas individuales. Por desgracia, Spectre y Meltdown son **vulnerabilidades de *hardware***, es decir, existen a nivel de *hardware*, por lo que es imposible remediarlas por completo con **parches de *software***.

Por consiguiente, se implementó uno de los parches en el núcleo del sistema operativo de Linux, pero ralentizaba mucho el sistema, por lo que un tiempo después se eliminó del código.

Spectre es conflictivo porque tiene como objetivo diferentes componentes de microarquitectura, por lo que se ha tenido que diseñar un parche aparte. Y cada uno de los parches requerirá que ciertas funciones estén desactivadas o que se realicen acciones adicionales, lo que disminuirá el nivel de rendimiento.

De hecho, los parches afectan tanto al rendimiento en muchos casos que un sistema parcheado funciona más lento que uno en el que los **componentes vulnerables del CPU** estén desactivados.

Por otra parte, debido a estas vulnerabilidades, ARM se vio en la necesidad de actuar frente a esto y promete **actualizaciones de *hardware*** y afirma que “todos sus CPU futuras serán resistentes a los ataques similares a Spectre”.

Estas son buenas noticias, pero en realidad no del todo, ya que la instalación de dichos parches causara estragos evidentes en el rendimiento, por lo que la solución podría no estar al alcance de todos.

Como ya fue mencionado, estas vulnerabilidades significan una gran amenaza, ya que abren la posibilidad a la filtración de información privada como contraseñas, datos bancarios ingresados e información personal, entre otros. Al ser estas vulnerabilidades que afectan es hardware, hace que evitarlo sea una tarea difícil y mucho mas para un usuario común, en otras palabras, se esta dejando al aire libre datos que podrían usarse de manera maliciosa.

Ejemplos de CPU's vulnerables

Spectre 1 afecta a procesadores Intel, ARM y también AMD.

Spectre 2 afecta a varios modelos ARM Cortex más actuales, ya que dispone de abreviaturas de las entradas BTB fácilmente predecibles por los atacantes.

Meltdown afecta a los ARM Cortex A-75.

Ejemplo

- Con Meltdown se puede robar contraseñas: El planteamiento es sencillo. En la ventana superior tenemos un gestor de contraseñas; nos pide la contraseña maestra para poder acceder al resto. Y en la ventana inferior, tenemos una terminal que ejecutará el código que se encargará de leer la memoria del gestor de contraseñas.

Lista de CPU’s vulnerables

Procesadores ARM afectados (Fuente: ARM)

Modelo	Variante 1 (Spectre)	Variante 2 (Spectre)	Variante 3 (Meltdown)	Variante 4 (Meltdown)
Cortex R-7	Si	Si	No	No
Cortex R-8	Si	Si	No	No
Cortex A-8	Si (bajo revisión)	Si	No	No
Cortex A-9	Si	Si	No	No
Cortex A-15	Si (bajo revisión)	Si	No	Si
Cortex A-17	Si	Si	No	No
Cortex A-57	Si	Si	No	Si
Cortex A-72	Si	Si	No	Si
Cortex A-73	Si	Si	No	Si
Cortex A-75	Si	Si	Si	No

Company	Spectre 1	Spectre 2	Meltdown
ARM	10 Mobile CPUs 3 Server SoCs	10 Mobile CPUs 3 Server SoCs	4 Mobile CPUs 3 Server SoCs

Vulnerables a ambos Spectre/Meltdown

- ARM Cortex-A75
- ARM Cortex-A72
- ARM Cortex-A57
- ARM Cortex-A15

Vulnerables a solamente a Spectre

- ARM Cortex-A17
- ARM Cortex-A12
- ARM Cortex-A9
- ARM Cortex-A8
- ARM Cortex-R8
- ARM Cortex-R7
- ARM Cortex-A73

Soluciones existentes o temporales para mitigar la vulnerabilidad de ARM sobre Spectre y Meltdown

Recordemos que ARM es solo el procesador, y en base a esto hay diferentes maneras de trabajar sobre estas vulnerabilidades que son dependientes del sistema operativo.

No existe una solución genérica para mitigar la vulnerabilidad, se deben aplicar los parches de seguridad liberados progresivamente por los fabricantes, la mayoría de estos cambios requieren un reinicio del sistema.

- **Microsoft:** Liberado el parche para windows 10, en el boletín del próximo martes 9 de enero serán liberados los parches para los demás sistemas operativos.
  Guía oficial de mitigación para Windows:
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

- **Actualización:** Microsoft ha liberado parches de emergencia a través del sitio oficial: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution-s

- **MacOS**: Solucionado desde la versión 10.13.2 para macOS High Sierra.

- **Android:** Google ha liberado los parches para dispositivos Pixel y Nexus, los demás modelos están sujetos a la liberación de parches por sus respectivos fabricantes.

- **Linux:** Parches disponibles, ejecutar proceso según la distribución.

- **Redhat** (CentOS, Fedora, Oracle Linux)
  sudo yum update
  sudo dnf update
  reiniciar el sistema
  sudo reboot

- **Debian** (Ubuntu / Mint)
  sudo apt-get update
  sudo apt-get update
  reiniciar el sistema
  sudo reboot

Conclusión

Las vulnerabilidades de ARM ponen en peligro la información que almacenamos dentro de los microcontroladores poniendo en riesgo desde información personal que se almacene de empleados o personas hasta la misma integridad de la tecnología que se haya creado. Por suerte la comunidad que utiliza estos procesadores se dio cuenta y no solo se tomó el tiempo de mostrar como atacar ARM, sino que también se tomó el tiempo de buscar diferentes soluciones y parches para evitar el robo de información que se puede usar en Meltdown y Spectre. En el caso de que se llegue a usar un procesar ARM tenemos la opción de consultar las tablas para revisar si los modelos con los que contamos son vulnerables y hasta qué grado.

Bibliografías

Perekalin, A. (2019). Las vulnerabilidades de Spectre y Meltdown en los CPU. ¿Qué depara el 2019? Recuperado de https://latam.kaspersky.com/blog/35c3-spectre-meltdown-2019/13925/

Rodriguez, D. (2018). Meltdown y Spectre | Vulnerabilidades críticas en Intel, AMD y ARM. Recuperado de https://shieldnow.co/2018/01/03/meltdown-y-spectre-vulnerabilidades-criticas-en-intel-amd-y-arm/

arm Developer. (s. f.). Arm Security Updates. Recuperado de https://developer.arm.com/support/arm-security-updates

Wong, Dr. A. (2018). Complete List Of CPUs Vulnerable To Meltdown / Spectre Rev. 8.0. Recuperado de https://www.techarp.com/guides/complete-meltdown-spectre-cpu-list/

Wong, Dr. A. (2018a). Apple, ARM & Intel CPUs Affected By Meltdown & Spectre. Recuperado de https://www.techarp.com/guides/complete-meltdown-spectre-cpu-list/4/#arm

ProjectBeta. (2018). Lista de procesadores ARM vulnerables a Spectre y Meltdown. Recuperado de https://noticias.top10games.es/noticias/lista-de-procesadores-arm-vulnerables/

Omicrono. (2018a). Así se puede usar Meltdown para robar contraseñas en tiempo real. Recuperado de https://www.elespanol.com/omicrono/software/20180104/puede-usar-meltdown-robar-contrasenas-tiempo-real/274723591_0.html

Delgado, A. (2018). Así son Spectre y Meltdown, las graves vulnerabilidades que afectan a Intel, pero también de manera limitada a AMD y ARM. Recuperado de https://www.geeknetic.es/Noticia/13084/Asi-son-Spectre-y-Meltdown-las-graves-vulnerabilidades-que-afectan-a-Intel-pero-tambien-de-manera-limitada-a-AMD-y-ARM.html