Meltdown e Spectre, i super bug del 2018 possono essere sfruttati in un vero attacco?

Author : Giuseppe Turano

Date : 31 luglio 2018

Il 3 gennaio del 2018 i ricercatori di Project Zero di Google, di Cyberus Technology, e dell'Università Tecnica di Graz hanno annunciato la scoperta delle due vulnerabilità di cui sono affetti la gran parte dei moderni processori utilizzati negli ultimi 20 anni.

I bug che hanno sconvolto il mondo hi-tech nel primo trimestre del 2018 sono Meltdown e Spectre. Oggi si conoscono tre variati di questi bug Variante 1 e Variante 2 (Spectre) e poi la Variante 3 (Meltdown). La Variante 1 (CVE-2017-5753) riguarda un problema di bounds check bypass, la Variante 2 (CVE-2017-5715) presta il fianco a una branch target injection e la Variante 3 (CVE-2017-5754) permette di accedere alla memoria cache della CPU in maniera inappropriata.

Queste vulnerabilità, sintetizzando al massimo il concetto e le metodologie con cui operano i moderni processori, permettono l'accesso diretto alla memoria delle CPU [1] e quindi ai dati in essa contenuti.

L'impatto di una simile notizia non poteva che essere devastante. L'insicurezza e l'incertezza che ha dominato il primo trimestre di quest'anno ha inevitabilmente messo a dura prova sia le grandi multinazionali dell'informatica che gli utenti finali.

Il sistema produttivo ha risposto con una febbrile corsa per rendere disponibili le patch[2] e aggiornare praticamente tutti i sistemi operativi (Windows, Linux, MacOS, Android, iOS). Mentre l'utente medio sembra si sia già dimenticato di quanto accaduto a inizio 2018.

Spectre, dal canto suo, è una vulnerabilità molto più difficile da contrastare. Spectre, non è legata direttamente a una singola falla software o hardware che sia, questa vulnerabilità si presenta non come un insieme di possibili vulnerabilità, qualcosa di indefinito, da cui il nome per intenderci, non tutte efficacemente risolvibili con patch software.

Spectre sarà risolto esclusivamente rivedendo le architetture hardware dei processori. Quindi il

primo consiglio è quello di diffidare o per lo meno di non prendere per certo il risultato dell'analisi degli innumerevoli tool di verifica che oggi infestano la rete.

L'analisi si riferisce solo alle sequenze note ma di suo Spectre può apparire sotto una molteplicità di sequenze impossibili da gestire.

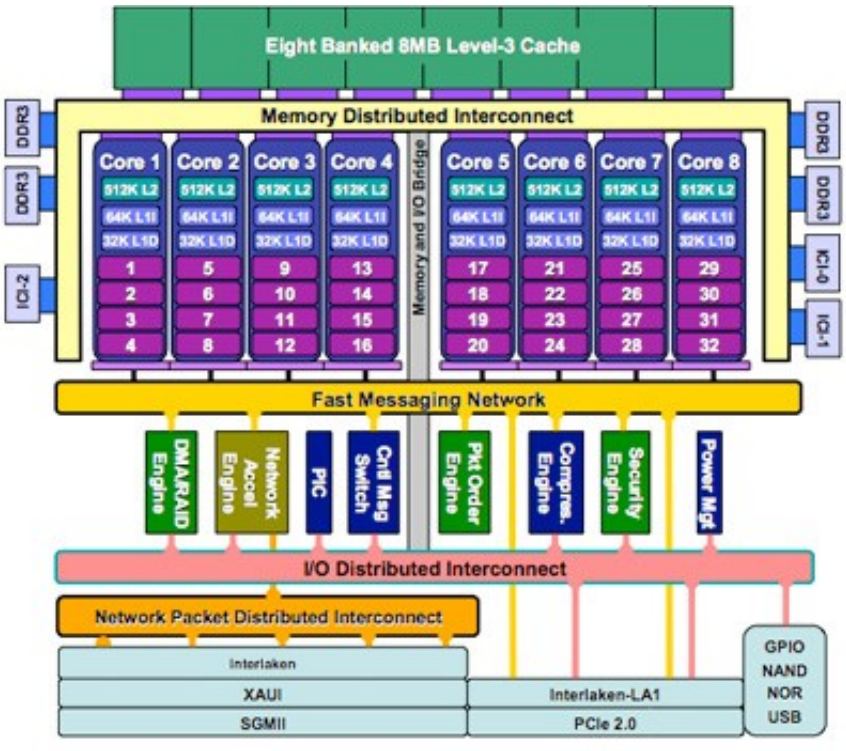
Come siamo giunti a questo punto?

A causa della necessità di migliorare le prestazioni dei microprocessori ottenuta in un primo momento aumentando la frequenza di calcolo della CPU. Oggi si è ormai giunti al limite fisico della tecnologia dei semiconduttori, ed aumentare ulteriormente la frequenza risulta sempre più difficile.

Perché arrenderci a un ostacolo fisico?

Per ovviare alle limitazioni fisiche dei semiconduttori si è inventato il Parallelismo[3].

La tecnologia dei semiconduttori consente di integrare in un solo chip più CPU facendole lavorare in parallelo. È immediato ipotizzare che si possa parallelizzare sia a livello di istruzione che a livello di CPU.



XLP832 Processor Block Diagram

Quello che interessa a noi in quest'articolo è che i processi di paralizzazione sono accompagnati da ulteriori meccanismi atti a velocizzare i processi di elaborazione dell'architettura creata. Tra tutte le tecniche utilizzate per migliorare le prestazioni delle CPU di

particolare interesse risultano essere:

1. La predizione di salto
2. L’elaborazione out-of-order e L’esecuzione speculativa

LA PREDIZIONE DI SALTO

In ogni programma informatico sono largamente presenti istruzioni di branch[4] che cambiano la sequenzialità delle istruzioni da eseguire. In presenza di branch quindi l’elaborazione in parallelo di una sequenza di istruzioni non può essere eseguita, e anche se eseguita a caso in una delle due direzioni del branch si rischia di dover azzerare la pipeline e le elaborazioni anticipate effettuate.

I moderni processori adottano delle tecniche di predizione del branch, provando a “indovinare” su base statistica il risultato della comparazione nel branch.

L’ELABORAZIONE OUT-OF-ORDER E L’ESECUZIONE SPECULATIVA

I moderni processori adottano architetture che contemplano sia tecniche di pipeline che superscalari. Questo porta già ad un buon livello di ottimizzazione.

Tuttavia, i programmi sono caratterizzati da istruzioni che dipendono dalle precedenti.

Al fine di massimizzare ulteriormente le prestazioni, i processori, nell’elaborare in anticipo le istruzioni, saltano temporaneamente quelle che hanno dipendenze dalle precedenti non ancora elaborate. Le istruzioni saltate sono lasciate in attesa e riprese successivamente quando la dipendenza può essere risolta.

Naturalmente l’esecuzione effettiva che segue viene realizzata sulla base dei risultati anticipati ma in modo da garantire la corretta sequenza.

Questa tecnica viene chiamata elaborazione Out-of-order.

La cosiddetta esecuzione Speculativa consente un ulteriore miglioramento delle prestazioni.

Consiste nell’anticipare il più possibile l'esecuzione di alcune parti del codice anche se non è certo che dovranno poi essere effettivamente eseguite, per la presenza ad esempio di un branch.

Adottando la tecnica di predizione di branch, con la tecnica speculativa viene anticipata l’elaborazione delle istruzioni nel ramo ritenuto più probabile.

MELTDOWN

Meltdown consente ad un attaccante di risalire al contenuto di zone di memoria riservate che non sono di competenza del proprio programma senza poterle modificare.

TARGET

Gran parte dei processori Intel e ARM degli ultimi 20 anni (anno di riferimento 2018).

REQUISITI

Essere in possesso di normali privilegi di un utente per eseguire un programma sulla macchina.

PROCESSO DI RIFERIMENTO

Normalmente il tentativo da parte di un processo di accedere ad una zona di memoria riservata provoca la generazione di una eccezione e quindi il fallimento della lettura dei dati.

L’istruzione che tenta di accedere ad una locazione riservata, come ogni istruzione, viene schedulata dalla pipeline della CPU. Al momento della esecuzione l’indirizzo di memoria da leggere viene inviato al gestore della memoria e qui il controllo dei privilegi di accesso fallirà, generando un’eccezione. L’istruzione non viene completata e il processo interrotto.

Benché i dati dalla memoria riservata sono stati effettivamente letti dal processore l'istruzione è stata interrotta prima del suo completamento e nessun dato è fornito al processo malevolo.

Questo meccanismo è da sempre ritenuto sicuro ed invalicabile.

DESCRIZIONE DELL’ATTACCO

Iniziamo con il porci una domanda. Dov’è finito il dato letto dalla CPU?

Il dato dalla memoria riservata e non consegnato al processo malevolo che voleva accedervi viene memorizzato nella cache del processore.

Facendo uso di alcune peculiarità del set di istruzioni x86, ed operando iterattivamente su ciascuna locazione di memoria, Meltdown consente di risalire e rivelare i dati di tutta la memoria mappata.

L’attacco viene eseguito in tre fasi:

1. fase inziale, viene effettuato un tentativo di lettura del valore segreto della locazione di memoria da attaccare creando un’eccezione

2. seconda fase, si indirizzano locazioni in cache con spiazzamenti basati sul valore segreto
3. fase finale l’attaccante utilizza la tecnica Flush+Reload per dedurre il valore segreto

Queste 3 operazioni possono essere ripetute per tante locazioni di memoria fino anche a ricavare il dump di tutta la memoria fisica.

DANNI PER GLI UTENTI

L’attaccante può accedere alla memoria fisica sottraendo:

- Documenti
- Foto
- password

SPECTRE

Spectre riesce a ingannare le applicazioni vulnerabili e ad accedere ai dati contenuti nella loro memoria.

TARGET

Processori Intel, AMD e ARM, e quindi anche in molti processori di Samsung e Qualcomm che sono basati su ARM e sono ampiamente utilizzati negli smartphone.

REQUISITI

Essere in possesso di normali privilegi di un utente per eseguire un programma sulla macchina.

DESCRIZIONE DELL’ATTACCO

L’attacco Spectre induce il processore della vittima ad elaborare in modo speculativo delle istruzioni che non sono eseguite nell’esecuzione corretta del programma lanciato.

Anche in questo caso abbiamo tre fasi per distinte

1. fase inziale di setup utilizzata per creare le condizioni che inducono in una fase successiva il processore ad elaborare istruzioni speculative utili per carpire informazioni. Nella fase di setup l’attaccante prepara anche il terreno per poi applicare la tecnica flush+reload oppure evict+reload.
2. seconda fase, il processore elabora le istruzioni speculative che modificano lo stato micro-architetturale.
3. fase finale l’attaccante utilizza la tecnica flush+reload o evict+reload deducendo l’informazione riservata misurando i tempi di accesso

DANNI PER GLI UTENTI

L’attaccante può accedere alla memoria fisica sottraendo:

- username
- password
- dati della navigazione web

CONCLUSIONI

Meltdown e Spectre impongono una profonda revisione delle architetture hardware dei processori (già si parla di nuovi schemi) e di conseguenza anche dei sistemi operativi.

Per entrambe le vulnerabilità la condizione fondamentale di non potere agire da remoto e i lunghi tempi dettati dalle iterazioni necessarie per effettuare il dump dei dati escludono per il momento l’utilizzo di queste vulnerabilità in un attacco informatico.

D’altro canto, qualsiasi dispositivo non monitorato e non aggiornato costituisce una falla in ogni infrastruttura informatica le vulnerabilità viste non fanno altro che allargare la superfice di bersaglio e costituisco una freccia in più nelle mani dei Cybercriminali.

FONTI:

- https://meltdownattack.com/
- https://spectreattack.com/spectre.pdf
- https://googleprojectzero.blogspot.it/2018/01/reading-privileged-memory-with-side.html
- *Intel Analysis of Speculative Execution Side Channels*
- Analyzing potential bounds check bypass vulnerabilities
- https://www.extremetech.com/computing/261792-what-is-speculative-execution
- https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability
- https://www.amd.com/en/corporate/security-updates
- Support Microsoft,

    https://support.microsoft.com/en-us/help/4073757/protect-your-windows-devices-against-spectre-meltdown
    https://support.microsoft.com/en-us/help/4078130/update-to-disable-mitigation-against-spectre-variant-2
    https://social.technet.microsoft.com/Forums/en-US/fd9f2f4f-2534-4d61-86cd-fa5f38ac1557/meltdown-and-spectre-must-registry-value-featuresettingsoverride-manually-set-after-patch
    https://docs.microsoft.com/en-us/cpp/cpp/spectre
    https://support.microsoft.com/en-us/help/4090007/intel-microcode-updates
- http://www.ictbusiness.it/cont/news/sbucano-due-nuove-varianti-di-spectre-le-cpu-tremano-ancora/41846/1.html
- https://blogs.vmware.com/euc/2018/02/meltdown-spectre-secure-end-user-computing.html

- http://www.brendangregg.com/blog/2018-02-09/kpti-kaiser-meltdown-performance.html

NOTE

[1] L'unità di elaborazione centrale (central processing unit, in sigla CPU, con particolare riferimento alla sezione logica in astratto) o processore centrale o più propriamente microprocessore (in sigla µP o uP, con particolare riferimento al chip hardware) è un tipo di processore digitale general purpose che si contraddistingue per sovrintendere a gran parte delle funzionalità del computer digitale basato sull'architettura di von Neumann o sull'architettura Harvard.

[2] In informatica una patch (in inglese pezza, toppa) indica una porzione di software progettata per aggiornare o migliorare un programma. Ciò include la risoluzione di vulnerabilità di sicurezza e altri bug generici.

[3] In informatica il calcolo parallelo è l'esecuzione simultanea del codice sorgente di uno o più programmi (diviso e specificamente adattato) su più microprocessori o più core dello stesso processore allo scopo di aumentare le prestazioni di calcolo del sistema di elaborazione.

[4] Un branch (salto o diramazione in alcune architetture di microprocessori, come il PDP-8 e l'Intel x86) è un punto nel quale in un processo viene alterato il sequenziale flusso delle istruzioni.

A cura di: **Giuseppe Turano**