Marco Dal Prà (m_dalpra)

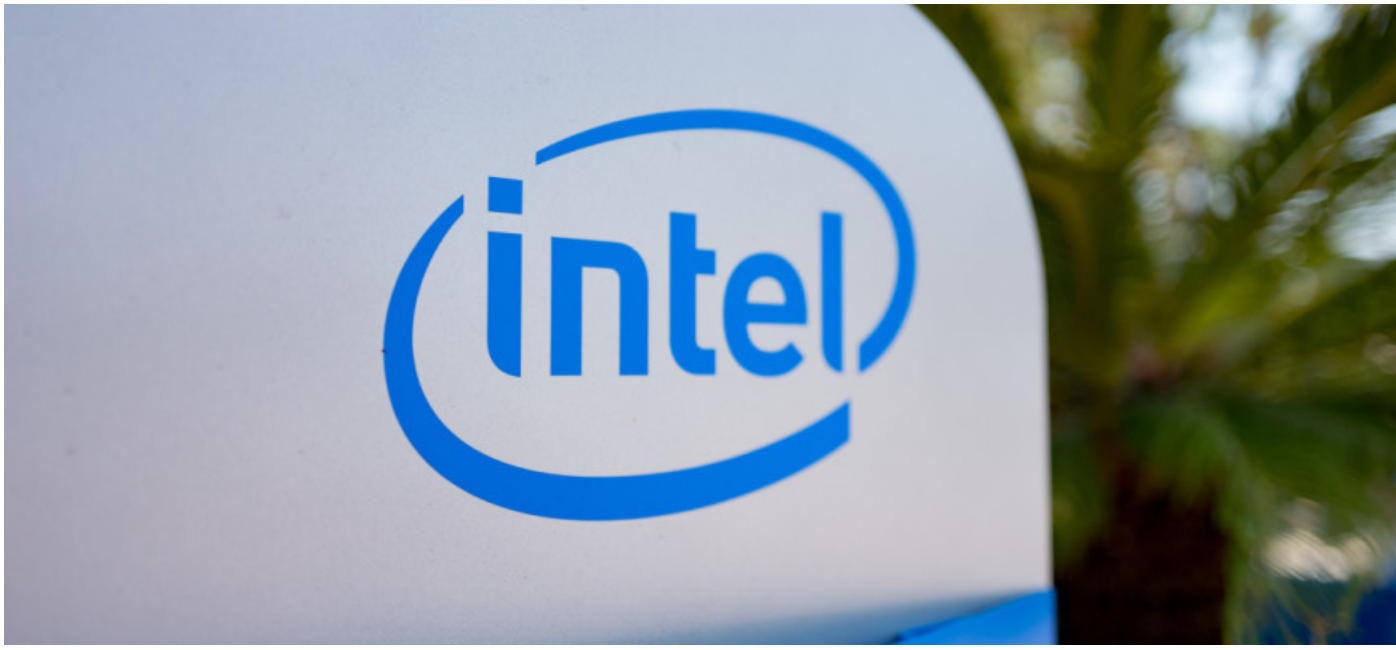
PERICOLOSO BUG SCOPERTO NEI MICROPROCESSORI

6 January 2018

E' una notizia che non vorrei mai voluto leggere. I ricercatori Google hanno trovato una falla nella parte Hardware dei microprocessori Intel che "distrugge" uno dei capisaldi della sicurezza di tutta l'informatica moderna : la Modalità Protetta. E' una notizia al limite dell'allucinazione : i computer da oggi sono dei colabrodo. Roba da non credere.

Piccola Premessa

La modalità protetta è una delle modalità in cui può funzionare una CPU Intel. Questa modalità di funzionamento fornisce direttamente un supporto all'esecuzione multipla dei programmi, **impedendo** che un programma possa accedere per errore all'area di memoria assegnata ad un altro programma [Wikipedia].



intel.jpg

La modalità protetta è stata per me una delle maggiori innovazioni dell'informatica degli anni '80, in cui frequentavo l'istituto tecnico. Consentiva al microprocessore di eseguire più programmi contemporaneamente "confinandoli", impedendo cioè ai programmi di invadere spazi destinati

ad altri, soprattutto quelli destinati al Sistema Operativo. Era praticamente la fine del DOS, quantomeno a livello concettuale.

Esecuzione Speculativa

All'incirca dal 1995 Intel (e altri a seguire), per aumentare le prestazioni dei microprocessori ha introdotto una caratteristica che si chiama "esecuzione speculativa", che in pratica consiste nell'esecuzione di programmi in anticipo rispetto a quanto richiesto, sperando che poi siano utili all'utente. Un modo di "preparare il campo", anche se potrebbe essere fatto inutilmente, perché poi il programma vero e proprio procede in modo diverso.
Una specie di gioco d'azzardo su quello che potrebbe succedere.
Ad esempio il processore potrebbe eseguire preventivamente sia il programma che scaturisce sia dalla pressione del tasto OK che quello del tasto ANNULLA, tenendo poi quello che effettivamente serve (ed abbandonando quello inutile).

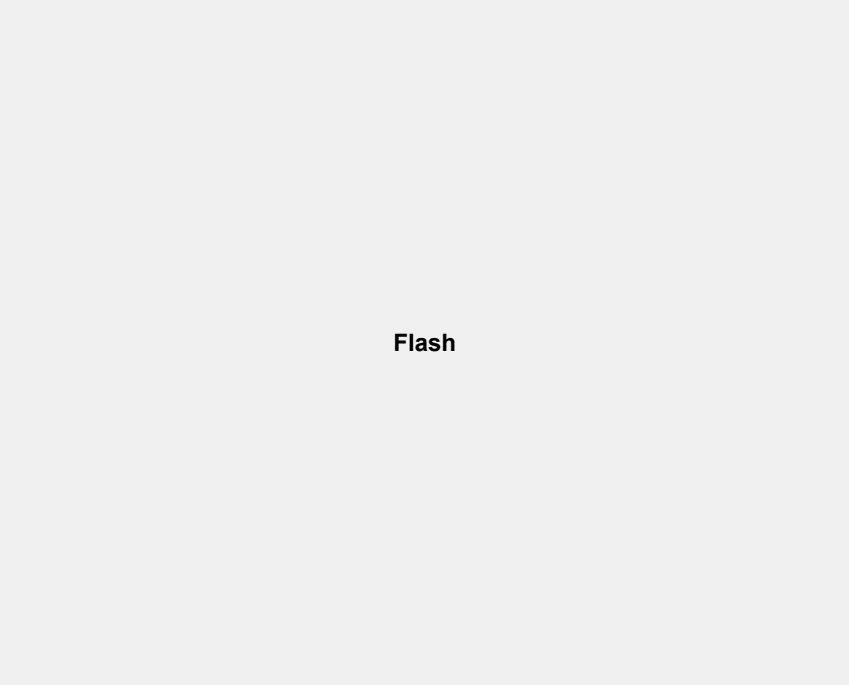
La scoperta di Google

Oggi si scopre che questa caratteristica fondamentale, intrinseca nell'hardware sia **Desktop che Portatili che Server** (inclusi quelli dei Cloud), ma **anche nei processori degli Smartphone**, ha un grave difetto, anzi direi una vera e propria falla.
Detta con semplicità, nelle aree di memoria "abbandonate" dall'Esecuzione Speculativa si potrebbe piazzare un programma "malevolo" il quale bypassando la modalità protetta può andare a spiare cosa c'è nella memoria del PC, senza dover rendere conto a nessuno. Libertà assoluta di accedere a qualunque informazione contenuta nella memoria fisica.
Dicono che NON se ne accorge nemmeno l'Antivirus !
Come se un cliente della banca potesse gironzolare dove vuole ed andare a vedere (indisturbato) cosa c'è in ciascuna cassetta di sicurezza.

meltdown-spectre bug

Un video allucinante

In questo video, fatto su di un PC con sistema operativo Linux (che, come risaputo è molto più sicuro e robusto di Windows), si vede come un programma "spione" potrebbe riuscire a leggere indisturbato la password che l'utente sta digitando nel riquadro superiore.



Quando ho visto questo video sono rimasto letteralmente sconvolto.
Dimostra che l'hardware non garantisce più nessuna sicurezza. E' la fine di quello che consideravo il "mito" dei moderni microprocessori, la modalità protetta, iniziata a tutti gli effetti nel 1985 con i processori Intel 80386.

Qualche Commento

Su questo problema si è esposto (preoccupato e polemico) anche Linus Torvalds, l'inventore di Linux, mentre sembra al limite del risibile la risposta di Intel "il problema esiste, ma è diffuso nell'industria e non è esclusivamente legato ai propri prodotti".
Come dire, lo sapevano tutti ma nessuno parlava, quindi siamo stati zitti anche noi.

Mali estremi Estremi rimedi

La notizia di questo "Bug" dei microprocessori sta rimbalzando nei siti di informatica e tecnologia di tutto il mondo, ma quello che traspare (e che mi sembra inevitabile) è che la soluzione definitiva a questo problema non si può trovare nel software (patch, Windows Update, Service Pack, ecc).
La soluzione del problema si ha solamente con la SOSTITUZIONE DEL MICROPROCESSORE !
Un po' come succede con i costruttori di automobili che richiamano i modelli affetti da qualche problema per sostituire un componente difettoso.
Ma qui... c'è da buttare via tutto il motore !

Conclusione

Non serve inventare Computer Quantistici per violare le misure di sicurezza: quelli sul mercato oggi sono già un colabrodo sufficiente per rubarvi tutto quello che avete senza che ve ne possiate nemmeno accorgere.

Il 2018 per l'informatica di tutto il mondo comincia proprio male.

AGGIUNTA DELL'ULTIMO MINUTO

Confesso di essere esageratamente pessimista.
Dalla lettura di questo articolo sembra che un pirata possa "rubare" qualunque informazione contenuta in un PC.
In realtà, dalle informazioni finora divulgate, la falla consente ad un programma (anche un Javascript che gira dentro un browser) di accedere alla memoria RAM, e quindi ai dati dei programmi **aperti in quel momento**.

Per l'hacker inoltre si presenta un problema : è vero che può scorrazzare dove vuole, ma la memoria dei PC è piuttosto grande; cercare qualcosa di utile potrebbe essere molto dispendioso in termini di tempo.
Ad esempio, se sta cercando le Password di Chrome o di Firefox, dovrebbe prima riuscire a capire **dove sono**, nelle centinaia di MegByte della vostra RAM.

Se posso dare un consiglio, prendete questo accorgimento quando usate il WEB Browser per accedere a siti internet che **hanno vostre informazioni piuttosto importanti e/o sensibili**.
I classici sono il sito della vostra Banca, la posta elettronica consultata con WebMail (come GMAIL), ed altri siti importanti in cui accedete mediante credenziali/password.
In tutti questi casi non aprite altri siti. Chiudete tutti gli altri programmi.
Prendete l'abitudine di chiudere le altre finestre e le altre sessioni del Browser.

Link Utili

- https://www.tomshw.it/bug-microprocessori-tutto-meltdown-spectre-90564
- Sito ufficiale del bug : https://meltdownattack.com/
- La notizia pubblicata da Google Project
- La notizia sul sito CNET.COM

Estratto da "http://www.electroyou.it/mediawiki/index.php?title=UsersPages:M_dalpra:sorprendente-bug-scoperto-nei-microprocessori"