Careless architectures cost security

Alessandro Barenghi

Politecnico Open unix Labs
Politecnico di Milano

alessandro.barenghi - at - polimi.it

5 aprile 2017

Careless architectures cost security

Personal computer

Dalla singola CPU alla federazione di calcolatori

- Necessità di scaricare la CPU da task impegnativi/secondari
- Coprocessori!
  - Da calcolo (i80x87, since 1977)
  - Gestione mem e I/O (i8042 , Gate A20 handler e tastiera, since 1982)
- Controller intelligenti! (SCSI, since 1981)

Personal computer

La legge (di Moore) è uguale per tutti

- Abbiamo $\approx 2^{23}$ volte più transistor per area disponibili
  - Le CPU crescono....
  - Coprocessori e integrati ausiliari ... anche!
- Nascita di northbridge e southbridge per gestire le periferiche a due velocità
- Integrazione del NB per ridurre la latenza (e perchè c' era posto...)

Scontro tra coprocessori e sicurezza

"chi vuole un bel DMA?"

- Il trasferimento mediato dalla CPU è così lento...
- Aggiungiamo la possibilità di copiare memoria bypassandola!
- IEEE 1394 a.k.a. Firewire può leggere/scrivere direttamente in RAM
  - Al punto da farla diventare una porta di debug[a]
- Apple Thunderbolt ha un comportamento simile

[a] https://lkml.org/lkml/2006/4/3/301

Dischi calcolanti

Controller molto intelligenti

- WD Green 2 TiB - 1 Cortex-M + 2 ARM926 @ 150 MHz, 64 MB DRAM[a]
- cfr: Requisiti di sistema di Doom (1993): CPU a 66 MHz, 8 MB RAM
  - Gli ARM 926s gestiscono a) porta SATA e cache, b) comunicazione con il resto del disco
  - Possono localizzare i dati nella cache
  - Cambiando il firmware (non firmato) potete intercettare/cambiare dati
  - e ... sì, ci boota su Linux :P

[a] https://spritesmods.com/?art=hddhack

Schede di rete calcolanti

Come "agevolare" la trasmissione dei dati

- Scheda di rete Gb Broadcom Netextreme BCM95701A10
  - CPU MIPS + DRAM per buffer pacchetti + Flash per codice
  - Supporta offloading di parte del TCP stack
- Il firmware originale la inizializza e termina la sua esecuzione
- Non direttamente in grado di leggere e scrivere arbitrariamente in memoria
  - Ma con qualche sforzo ci si riesce via DMA[a]
  - Risultato? Remote keylogger
- Nessuna firma digitale sul firmware, solo un CRC-32 (rotto)

---

[a] http://esec-lab.sogeti.com/static/publications/11-reconnicreverse_slides.pdf

La bella addormentata nel case

ACPI States

- S0 PC acceso, funzionante
- S1 Power-on-suspend: CPU accesa, registri/caches mantenuti, non pronta ad eseguire, RAM mantenuta, PSU accesa
- S2 Standby: CPU accesa senza contesto, RAM mantenuta, PSU accesa
- S3 Suspend-to-RAM: come sopra, con una refresh rate più bassa per la RAM
- S4 Suspend-to-Disk: sistema spento, contesto copiato su disco, svegliabile via WOL/WOR, riprende dallo stato precedente
- S5 "Soft-off": "spento", PSU collegata
- S6 Non ACPI ufficiale: spento, PSU staccata

Going full coprocessor

Cos'è che...

- Tiene in piedi un webserver con TLS?
- É in grado di comunicare via ethernet, wi-fi?
- É in grado di riconoscere comandi vocali?
- Funziona con pochissima energia?

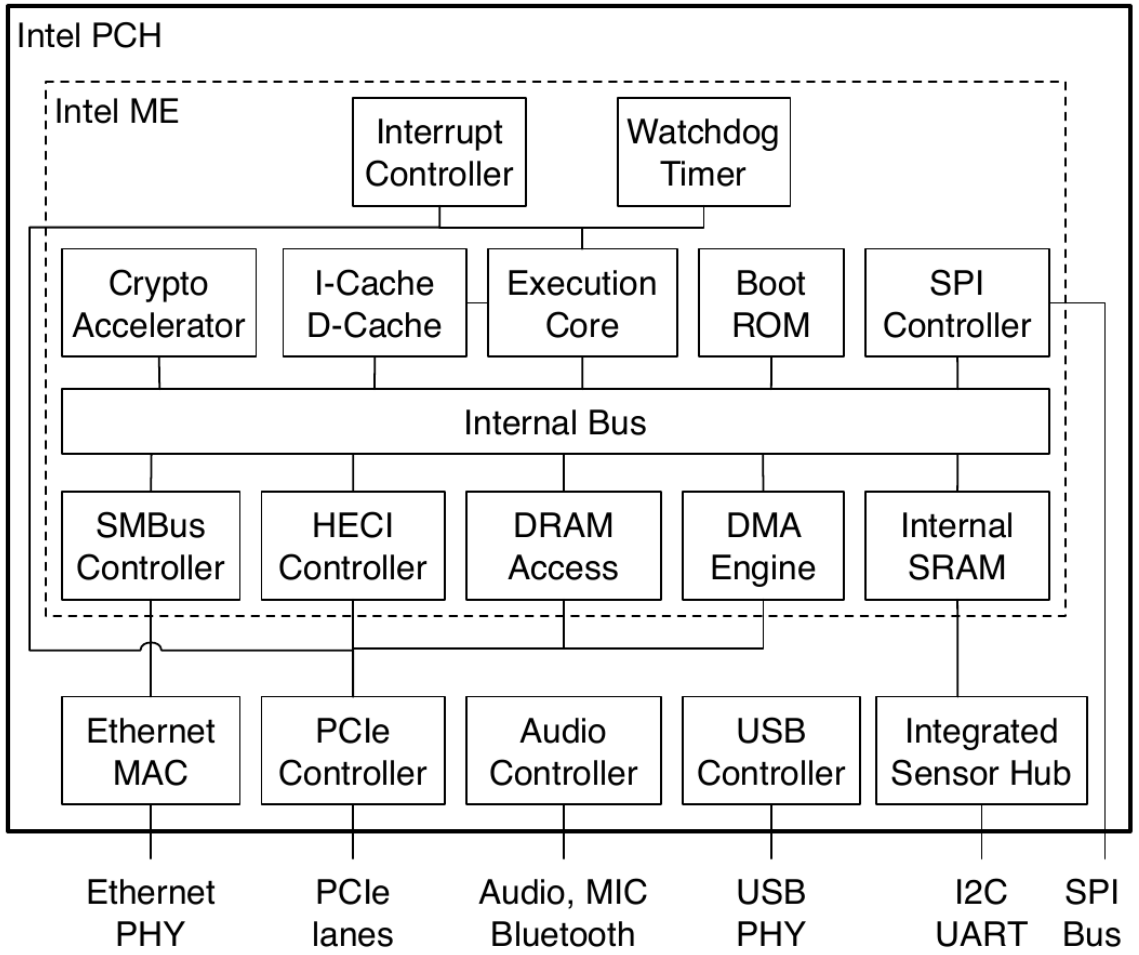
Intel vPro

Come gestisco il mio PC da remoto?

- Basato su combinazione di componenti nel southbridge + sw
- Presente dalla generazione Core2 di Intel[a]
- Sempre responsivo (anche in S6), è in grado di
  - Spegnere/Accendere/Riavviare la macchina da remoto
  - Redirigere tastiera/mouse in remoto
  - Avere un log di eventi in una memoria dedicata $\neq$ hdd
- Parte del sw stoccato su una ROM dedicata, parte sulla stessa Flash del bios

[a] http://download.intel.com/pressroom/kits/vpro/McCrearyMontevinaTechnicalWP.pdf

Intel Management Engine



[1]

[1] https://eprint.iacr.org/2016/086.pdf

Intel Management Engine

Cosa può andare storto?

- C'è un intero calcolatore nascosto in un chipset, con periferiche proprie, e accesso senza restrizioni al PC ...
- Il blob binario non è facilmente ispezionabile
  - Compressione huffman con dizionario non noto
  - Dopo un po' di sforzi, è stato ricavato a manina
- Iniezione di codice: nel 2009 proof-of-concept per Intel Q35[a]
  - Fix introdotto da Intel nella generazione successiva, e con updates per la precedente...
  - Ma l' ME può forzare roll-back del BIOS, prelevando la copia da remoto

[a] https://invisiblethingslab.com/resources/bh09usa/Ring%20-3%20Rootkits.pdf

Intel Management Engine

Fa anche altro?

- Il ME ha un ruolo di supporto nel bootstrap della CPU

Allora non posso toglierlo?

- Nel senso di eliminare fisicamente il componente HW: no.
- Posso agire sul SW?: Sì
  - Indagando su come ME carica il SW contenuto nella Flash del BIOS/EFI si scopre che è possibile rimuovere la stragrande maggioranza dei moduli
  - ME Cleaner[a] è in grado di ripulire un'immagine del BIOS

[a] https://github.com/corna/me_cleaner

Ferro al servizio della sicurezza

Dopo velocità e consumi...

- Avendo “abbastanza” efficienza per gli usi comuni
  - Intel SGX
  - AMD SME SEV
  - ARM TrustZone / MIPS prpl

Intel SGX

Compartimentazione per processo

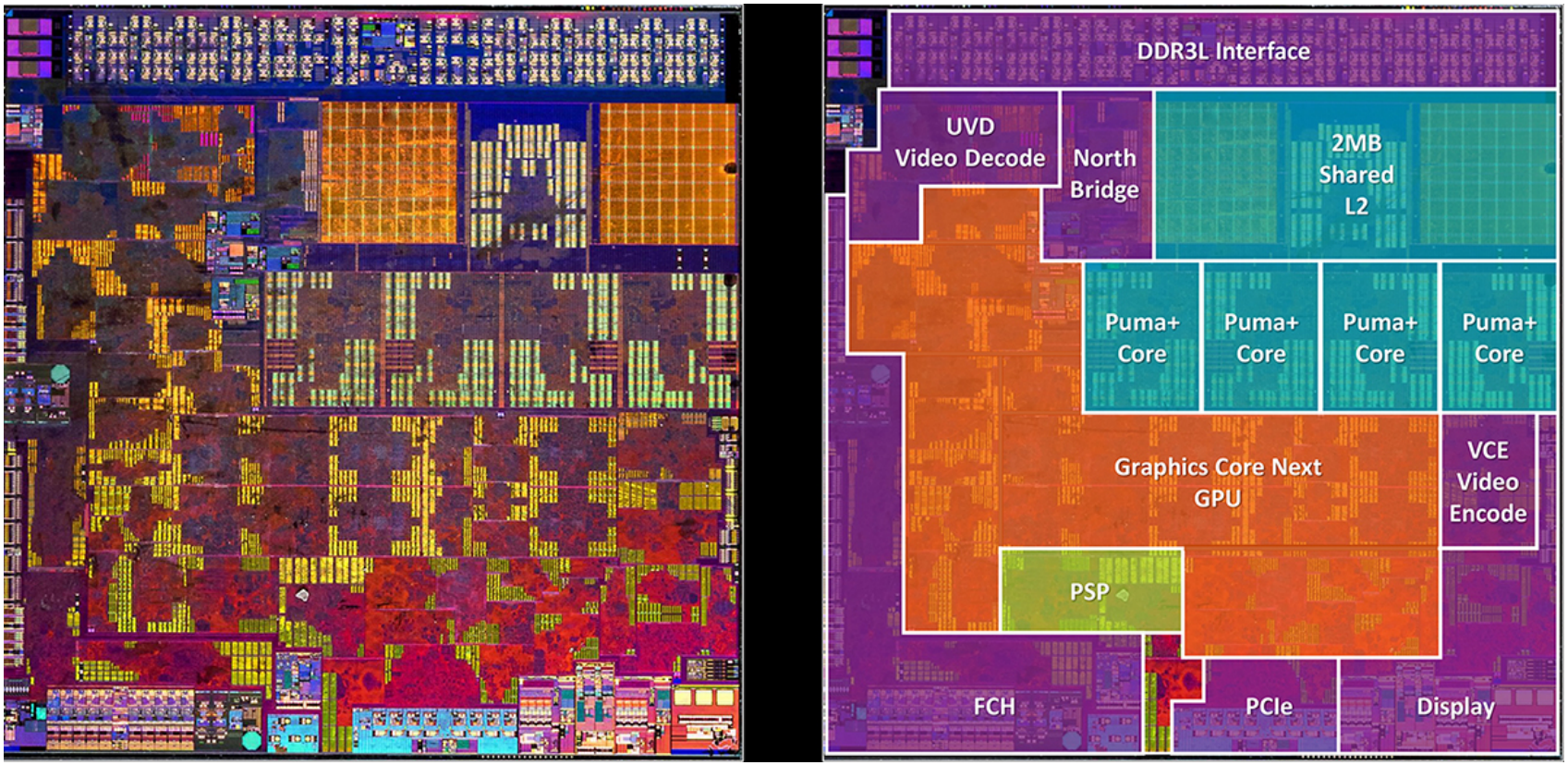
- Dati di un processo non accessibili (neppure dall'OS)
  - Intel non dà dettagli estremamente accurati, cifrata con AES
- Ufficialmente sostenuta dal Management Engine
  - Molto probabilmente per la parte di key management
- Supporta attestazione remota del codice
  - Intel agisce come trusted third party
  - É necessario "telefonare a casa"
- Descrizione approfondita in
  `https://eprint.iacr.org/2016/086.pdf`

AMD Platform Security Processor

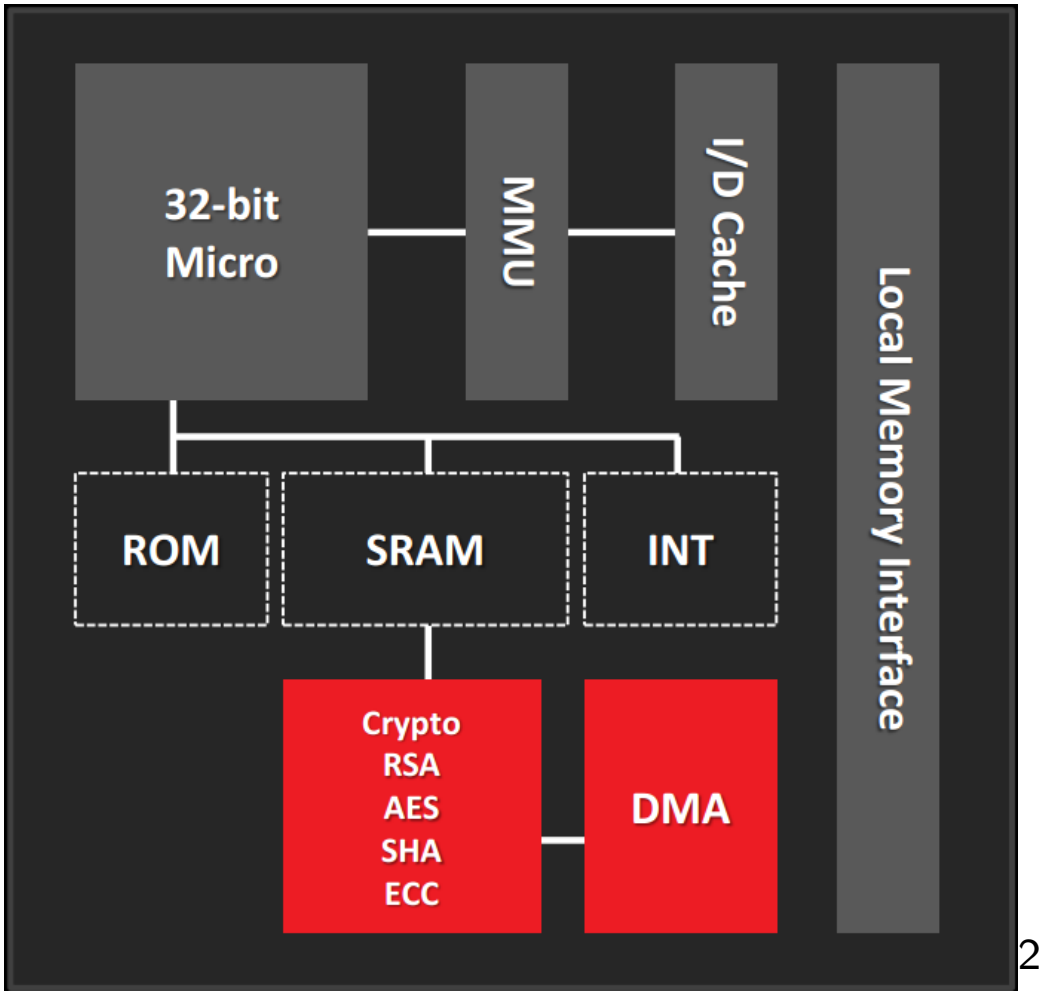
Una smart-card on die

- Nel 2013 AMD ha la necessità di ricevere il bollino Windows compliant
  - Ovvero le serve avere una catena di boot trusted
- I sistemi AMD based non sono dotati di un chipset intelligente come quello di Intel (= non hanno ME)
- AMD include una CPU con memoria e coprocessore crittografico dedicato con l' unico scopo (noto) di controllare la firma del BIOS

AMD PSP: dove?


DDR3L Interface
UVD
Video Decode
North
Bridge
2MB
Shared
L2
Puma+
Core
Puma+
Core
Puma+
Core
Puma+
Core
Graphics Core Next
GPU
VCE
Video
Encode
PSP
FCH
PCIe
Display

AMD PSP: cosa?



[2]

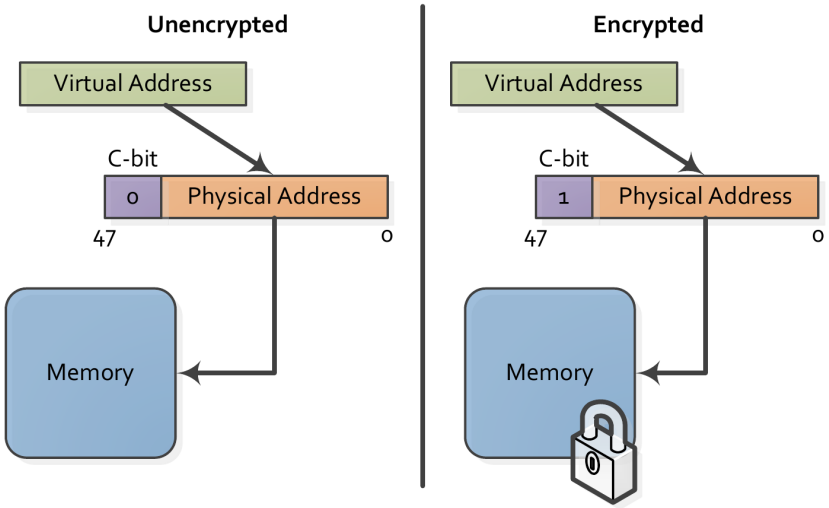
[2] Credit: AMD UEFI plugfest 2013 slides

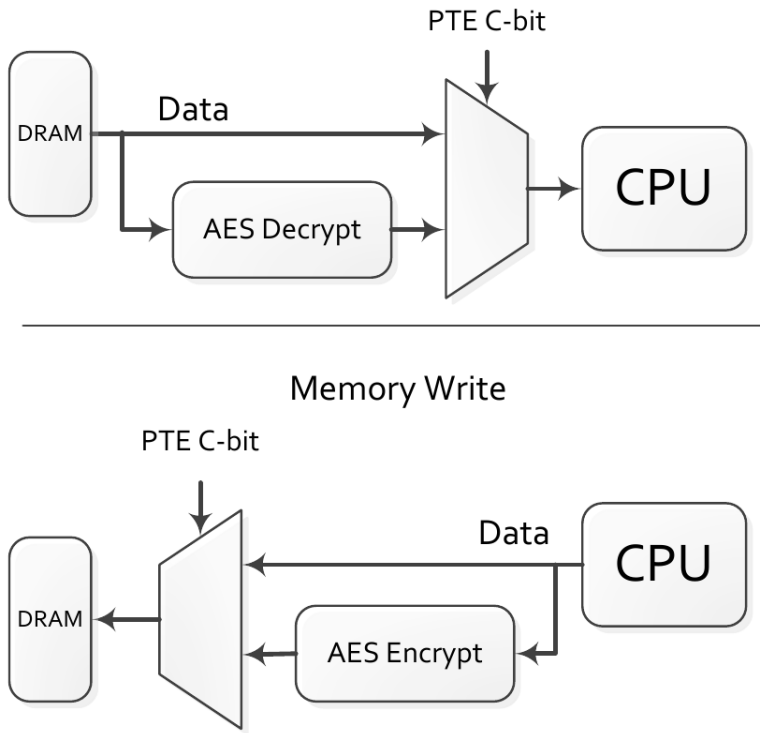
AMD Platform Security Processor

AMD Ryzen

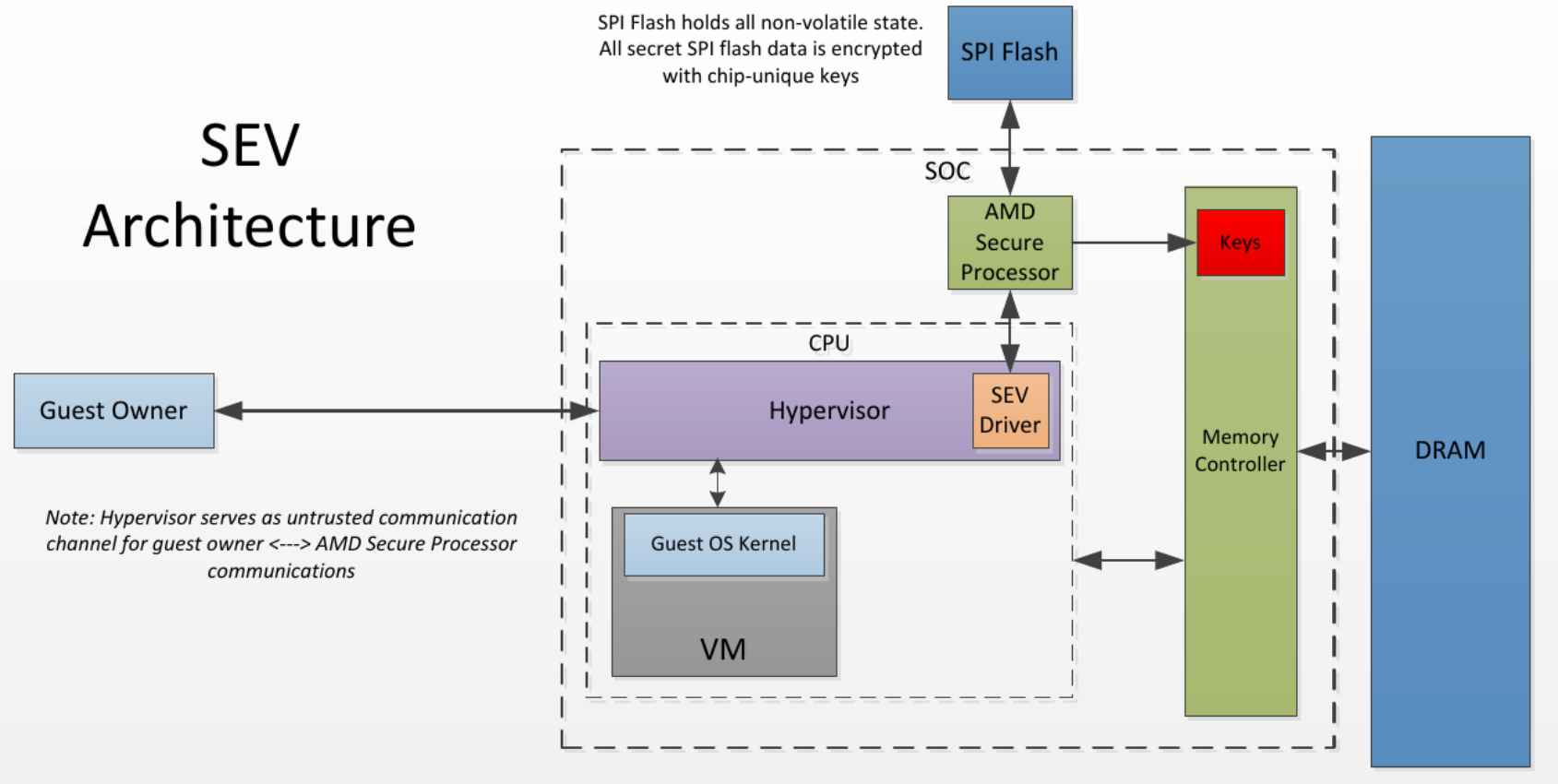
- Dopo 3 anni (abbondanti) di iato nel design architetturale AMD presenta i nuovi processori con architettura Zen
- Il PSP, una volta esclusiva di quelli a basso consumo, è presente su tutti
- É ancora ferro (quasi) morto? Fortunatamente no
  - Secure Memory Encryption
  - Secure Encrypted Virtualization

AMD SME


Unencrypted
Virtual Address
C-bit
0
Physical Address
47
0
Memory
Encrypted
Virtual Address
C-bit
1
Physical Address
47
0
Memory


PTE C-bit
DRAM
Data
AES Decrypt
CPU
Memory Write
PTE C-bit
Data
CPU
DRAM
AES Encrypt

AMD SEV


SEV
Architecture
SPI Flash holds all non-volatile state.
All secret SPI flash data is encrypted
with chip-unique keys
SPI Flash
SOC
AMD
Secure
Processor
Keys
CPU
Guest Owner
Hypervisor
SEV
Driver
Memory
Controller
DRAM
Note: Hypervisor serves as untrusted communication
channel for guest owner <---> AMD Secure Processor
communications
Guest OS Kernel
VM

Conclusioni

That's all folks

Domande?