HÁLÓZATI RENDSZEREK ÉS SZOLGÁLTATÁSOK TANSZÉK

MŰEGYETEM 1782

Budapest,
2024.05.22.

SZÁMÍTÓGÉP ARCHITEKTÚRÁK

Támadások a spekulatív végrehajtás ellen

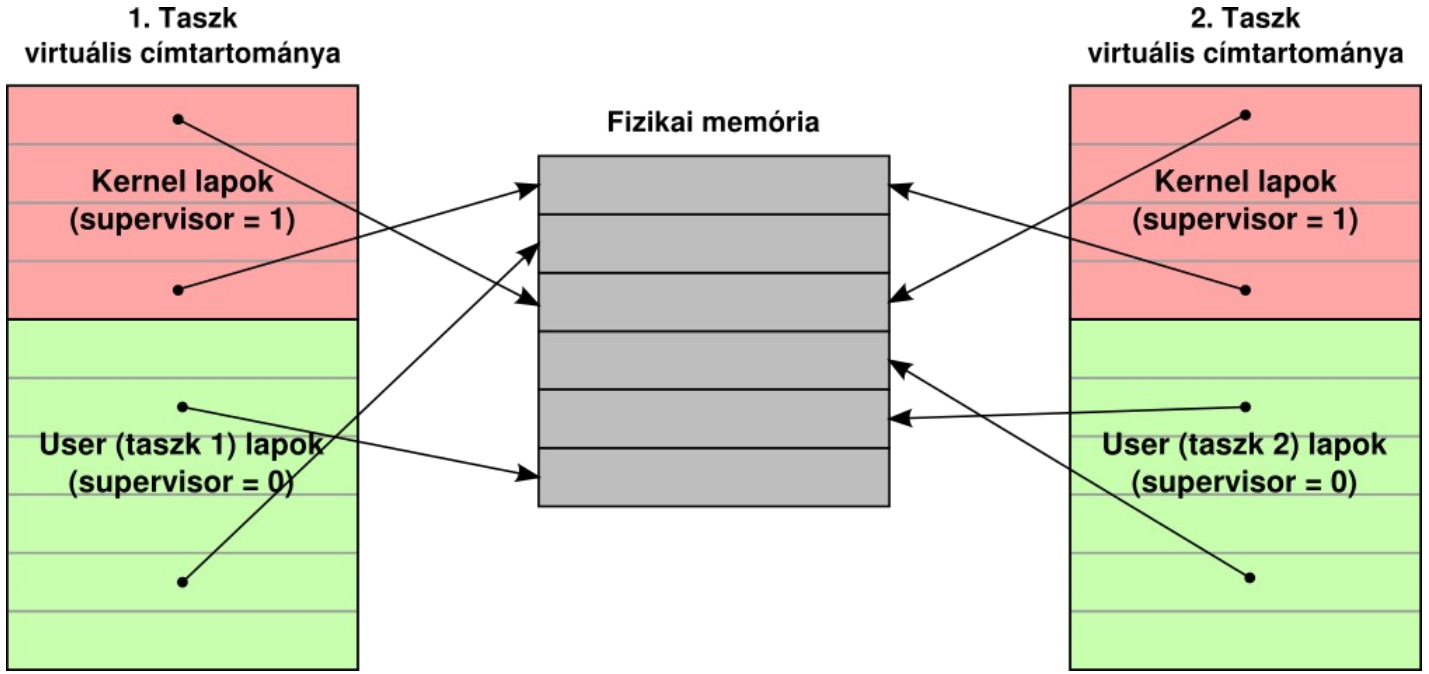
Horváth Gábor, Belső Zoltán

BME Hálózati Rendszerek és Szolgáltatások Tanszék
ghorvath@hit.bme.hu, belso@hit.bme.hu

Hozzávalók

USER ÉS KERNEL LAPOK

- Ismétlés: minden taszk külön laptábla
  - Taszk váltás → laptábla váltás
- Amiről nem beszéltünk:
  - A taszkok laptáblái tartalmazzák a kernel címteret is
  - Hogy a kernelt gyorsan lehessen hívni
  - … de ezeken a lapokon a „supervisor” bit=1 → csak a kernel éri el



USER ÉS KERNEL LAPOK

- User taszk:
  - Csak a saját lapjait éri el
- Kernel:
  - A taszk és kernel területet is eléri
- Kernel hívás:
  - User taszk egy speciális megszakítással hívja a kernelt
    - EAX regiszterbe tesszük a kívánt kernel funkció számát
    - Linux: `INT 0x80`, Windows: `INT 0x2e`
  - Megszakításkor CPU automatikusan user → kernel módba vált
  - Elérhetők lesznek a kernel lapok is
  - Kernel hívás végén visszavált user módba

SPEKULATÍV VÉGREHAJTÁS

- Spekulatív végrehajtás =
  olyan utasítás hajtódik végre, ami lehet, hogy nem is szükséges
- Két megjelenési formája:
  - Elágazásbecslés
    - Rossz becslés: téves utasítások „invalidálása”
  - Kivételkezelés
    - Kivétel fellép: a tévedésből elkezdett utasítások „invalidálása”
- Invalidálás jelentése:
  - Téves utasítások eredményének eldobása
    - Az architekturális állapot szintjén
  - … ennyi nem mindig elég !!! Nyomtalanul el kellene tűnnie!
    - Mikroarchitekturális állapot nem mindig visszaállítható
    - Nyomot hagyhat cache-ben, TLB-ben, BTB-ben, stb.
    - Szerencsére ezek nem elérhetőek (biztos?)

IDŐMÉRÉSES TÁMADÁSOK

- = side channel attack
- = próbálgatunk és mérünk

- N karakteres jelszó törése
  26^N helyett 26·N lépésben:
  - Próbálgatunk: Ax, Bx, Cx, …, Zx
  - Mérjük a reakcóidőt
  - Tovább tart a válasz, ha eltaláltuk az első betűt
    - Strcmp-nek a másodikat is meg kell néznie!
  - Továbblépünk a második betűre, stb.

Meltdown

ELVEK

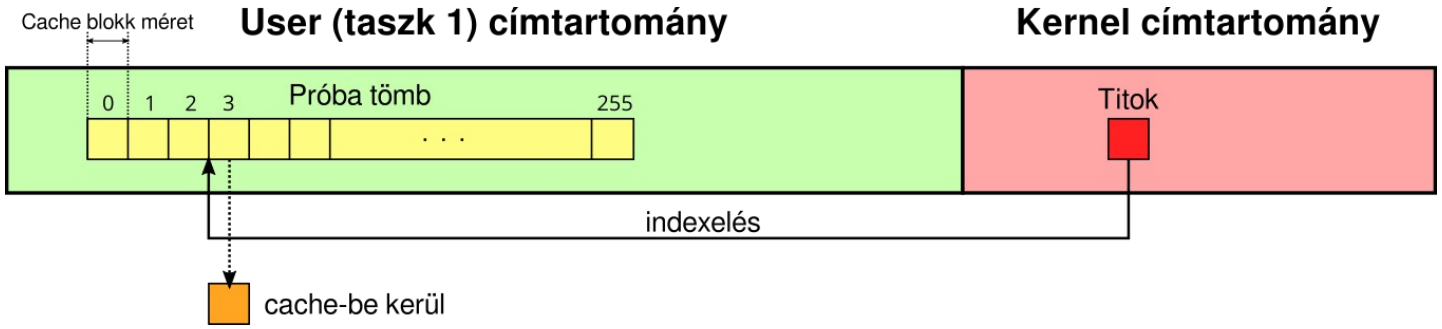
- A probléma gyökere:
  - A támadó kihasználja a spekulatív végrehajtást
  - Spekulatív utasítások mikroarchitekturális nyomot hagyhatnak
  - Ezt kihasználva elérhető a kernel memória

- Ötlet:
  - Próbáljunk meg elérni kernel adatot (titkot)
  - Nem fog menni (védelmi hiba)
  - De az adatelérés lefuthatott, mielőtt a védelmi hiba kiderül
  - Persze invalidálva lesz, de a cache-ben nyoma marad
  - … ezt használjuk ki!

MEGVALÓSÍTÁS

- Kernel titok, amit el akarunk érni: „titok”

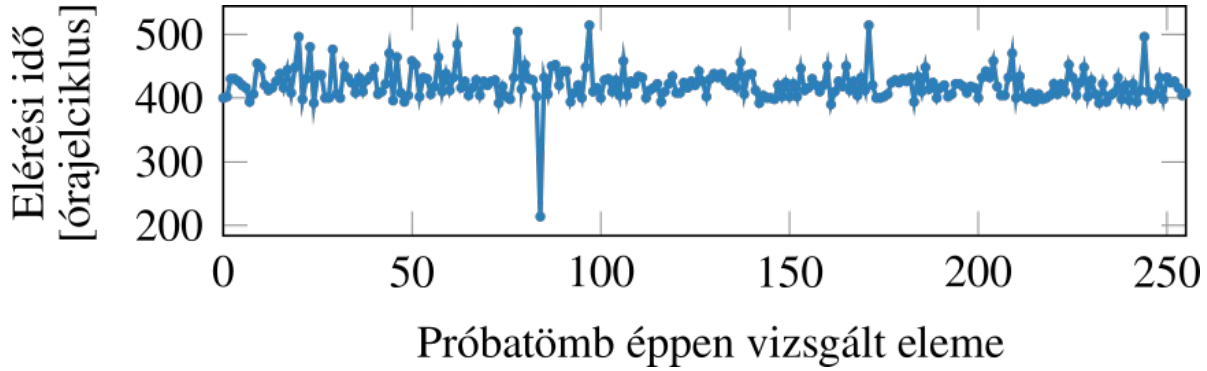
```
i1: R1 ← MEM[titok címe]
i2: R2 ← R1 * 64
i3: R3 ← MEM[proba + R2]
```



- i1: védelmi hibát okoz, nem hajtódik végre tovább a program
- De a hiba csak később derül ki
- i2, i3 invalidálásra kerül (R1, R2, R3 nem változik)
- **De a próba tömb R1-edik eleme a cache-be került!**

MEGVALÓSÍTÁS

- **A próba tömb R1-edik eleme a cache-be került!**
  (miközben a tartalma persze nem változott)
- A próba tömb elemei 64 byte-osak
  → minden R1 értéknél más blokk kerül a cache-be
- Kimérhetjük, mi lehetett R1!
- Végigmegyünk a próba tömbön, és mérjük az elérési időt:



→ R1 értéke 84 volt

GYÓGYMÓD

- Kernel memória 100-500 KB/s sebességgel dumpolható
- KPTI (KASLR, KAISER)
  - Kernel lapokat nem tesszük a user taszk laptáblájába
  - → Kernelhíváskor is laptáblát kell váltani
  - Akár 30% overhead is lehet
  - AMD CPU-k nem érintettek

EGYÉB TÁMADÁSOK A SPEKULATÍV VÉGREHAJTÁS ELLEN

- Meltdown (2017):
  - A kivételkezelés működését használja ki
  - A taszk saját laptábláján keresztül ér el adatot jogosulatlanul
  - Könnyen gyógyítható (≈)
- Spectre (2017):
  - Feltételes elágazás miatti spekulatív végrehajtást használja ki
  - Cél: a CPU rábírása, hogy spekulatívan végrehajtson egy általunk választott kódot egy idegen címtérben
    - Spectre v1: ugrási feltétel becslése érintett
    - Spectre v2: ugrási cím becslése érintett (BTB szándékos „félretanítása”)
  - Idegen taszk laptábláján keresztül jut titokhoz
  - Nagyon nehezen kezelhető
- Sorra derül fény egyéb, spekulatív mechanizmusok támadhatóságára!

HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK