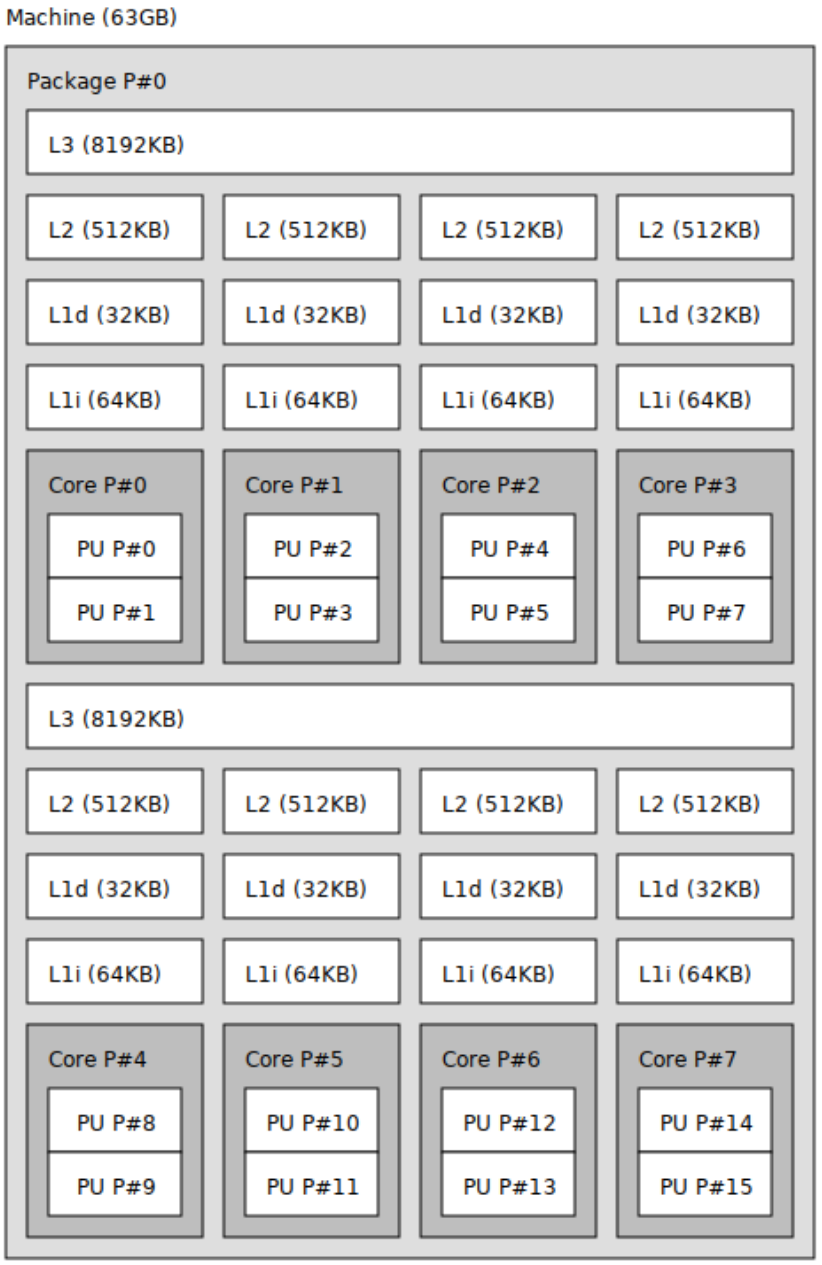
Spectre und Meltdown

Linux-Workshop Köln
9. Januar 2018

Harald Weidner
hweidner@gmx.net

Topologie eines Prozessors



- Ausgabe von **lstopo** (Ubuntu / Debian: Paket hwloc)
- Hier: AMD Ryzen 7 1700

- Zugriff auf L1 Cache in 1 Taktzyklus
- Zugriff auf RAM: ca. 100-150 Taktzyklen

Out-of-order Architektur

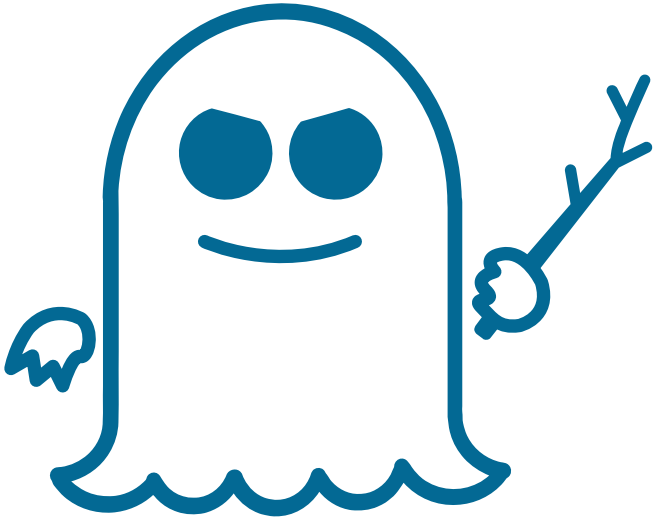
- Intel: seit Pentium Pro (1995)
- CPU ändert die Reihenfolge der Instruktionen, um Geschwindigkeitsvorteile zu erzielen
  - Hauptursache: Warten auf RAM-Zugriffe
  - Änderung darf Gesamtergebnis nicht verändern
- Varianten:
  - Speculative Execution
  - Branch Prediction
  - Im Falle eines Irrtums: vollständiges Zurückrollen aller Änderungen

Seitenkanal-Angriff

Angriff auf internen Zustand einer Schaltung / eines Programmteils durch Beobachten / Messen von

- Laufzeitverhalten
- Stromverbrauch
- Wärmeentwicklung
- Elektromagnetische Abstrahlung

Spectre



- Fehler:
  - RAM-Inhalt, der während speculative execution gelesen wird, füllt den Cache
  - Cache nach irrtümlicher Ausführung nicht gelöscht
  - Durch Timing-Angriff nachweisbar
- In CPUs von Intel, AMD, ARM, Oracle, IBM, …
- Nur im selben Prozessraum, schwer auszunutzen
- Bekannte Exploits über eBPF(-JIT), Javascript

Meltdown

- Fehler:
  - CPUs erlauben ansonstene verbotene Speicherzugriffe während speculative execution
  - Im Irrtumsfall werden Ergebnisse verworfen, aber Cache-Seiteneffekte bleiben bestehen
- Fehler in vielen Intel- und einigen ARM-CPUs
- Gegenmaßnahme: KAISER / KPTI Patche (Linux 64 Bit) mit z.T. erheblichen Performance-Verlust

History

~1995	Seitenkanalangriffe werden Forschungsthema
2012	Vortrag bei Intel zu Seitenkanalangriffen auf aktuelle CPU Designs
Juni 2017	Team bei Google Project Zero findet Schwachstellen und informiert Hersteller
Juli 2017	Veröffentlichungen von TU Graz und Blogbeitrag von G Data
Nov. 2017	KAISER / KPTI Patches
Jan. 2018	Veröffentlichung des Register

Quellen

- Veröffentlichungen der TU Graz et.al.
  https://meltdownattack.com/

- Google Project Zero
  https://googleprojectzero.blogspot.de/2018/01/reading-privileged-memory-with-side.html

- Artikel im Register
  https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/