Wait a minute for RISC-V Cross-core cache attack on a real-world SoC

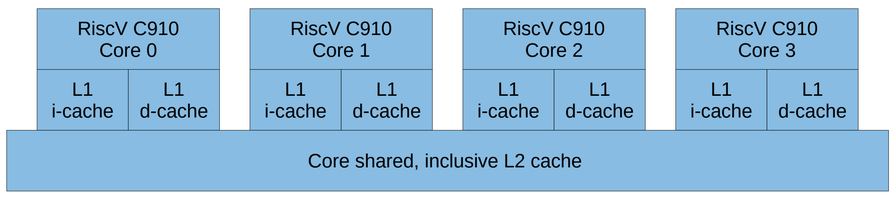
Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Kilian Zinnecker, Dr. Nisha Jacob Kabakci, Andreas Seelos-Zankl

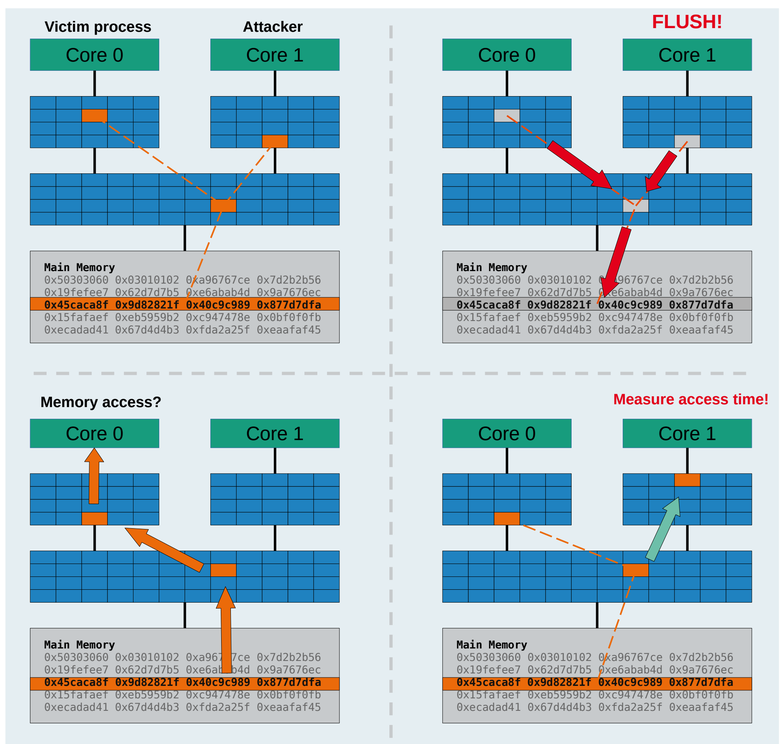
Demonstration of a known cross-core cache side-channel attack on a real world RISC-V SoC, running a contemporary OpenSSL RISC-V implementation of AES.

Target SoC cache architecture: Quad-core C910



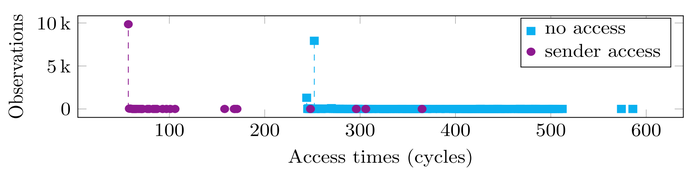
- Real world SoC based on quad-core C910 RISC-V CPU
- L2 cache is unified, **core shared** and **inclusive**
- Vendor ISE specific low-privilege cache flush instruction can be misused for FLUSH+RELOAD [1]

FLUSH+RELOAD [2]
Known cache attack on inclusive caches



1. Attacker flushes target cache line from cache
   → Inclusiveness causes flush from all cache levels
2. Attacker waits for victim to execute
3. Attacker measures own access time to target cache line
   → fast access: Victim accessed cache line meanwhile
   → slow access: No access by the victim meanwhile

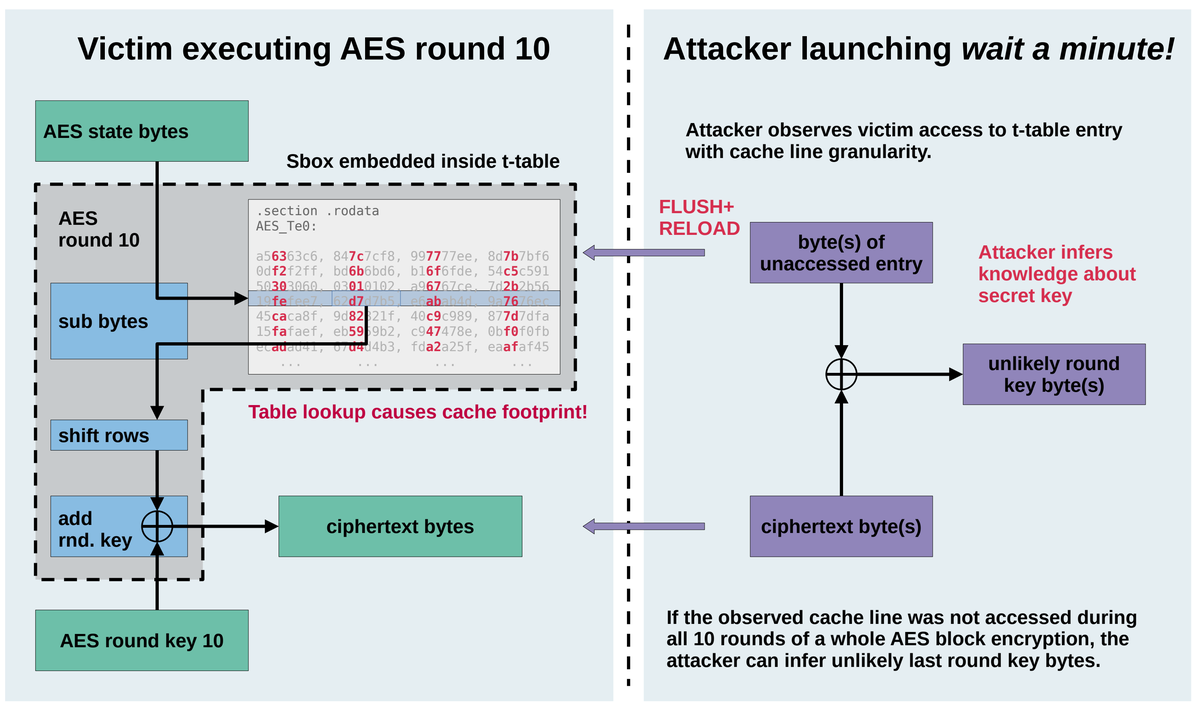
→ Attacker infers victim's memory access patterns!



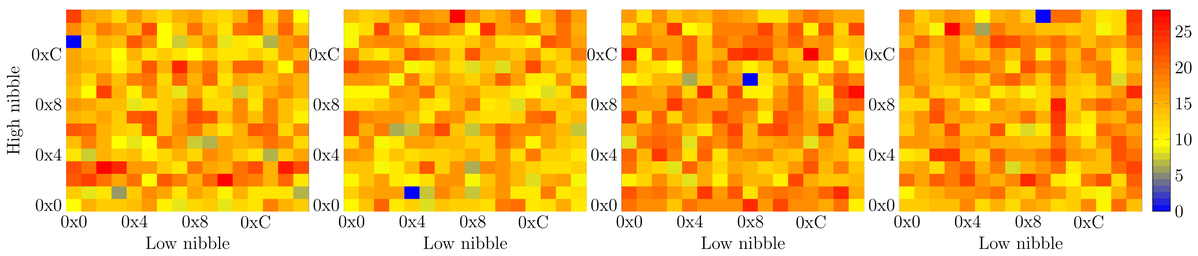
FLUSH+RELOAD timings measured cross-core on target SoC

Wait a minute! attack on AES T-table implementation [3]

- Known ciphertext attack against AES T-table implementation, using FLUSH+RELOAD
- T-tables: large lookup tables, with fixed, precomputed values to speed-up AES, residing in shared memory
- T-tables likely found in field, as target SoC does not feature any crypto extensions
- **Recent OpenSSL features AES T-table implementation optimized for RISC-V** [4]



Principle of the Wait a minute! attack



After multiple measurements the unlikely round key bytes can be exluded, indentifiying the last round key bytes thus the secret key

Conclusion

With regard to security, known problematic design choices were made again.

What can be done about it?

- Don't introduce low privilege cache flush instruction in ISE [1].
- **Disable cache flush instruction on affected SoC** [5].
- Adopt **crypto extensions** to prevent use of AES t-table implementation or use more secure software implementations.
- **Beware of security implications of microarchitectural design choices.**

1. Lukas Gerlach et al. A Security RISC: Microarchitectural Attacks on Hardware RISC-V CPUs. IEEE S&P 2023. 2023. doi: 10.1109/SP46215.2023.10179399.
2. Yuval Yarom and Katrina Falkner. FLUSH+RELOAD: A High Resolution, Low Noise, L3 Cache Side-Channel Attack. USENIX 2014. 2014.
3. Gorka Irazoqui et al. Wait a minute! A fast, Cross-VM attack on AES. RAID 2014. 2014. doi: 10.1007/978- 3-319-11379-1_15.
4. Add AES implementation in generic riscv64 asm. https://github.com/openssl/openssl/commit/b60603c5e3ac6396306bbaafd829f8340d22e1a0. 2022.
5. XuanTie-Openc910-UserManual. Version 03. T-Head Semiconductor Co., Ltd. https://occ-intl-prod.oss-ap-southeast-1.aliyuncs.com/resource/XuanTie-OpenC910-UserManual.pdf.

RISC-V Summit Europe 2024