RISCover: Automatic Discovery of User-exploitable Architectural Security Vulnerabilities in Closed-Source RISC-V CPUs

GhostWrite

Fabian Thomas, *Eric García Arribas, Lorenz Hetterich, Ruiyi Zhang, Daniel Weber, Lukas Gerlach, Michael Schwarz*

ACM CCS '25

Open Standard, Closed Chips

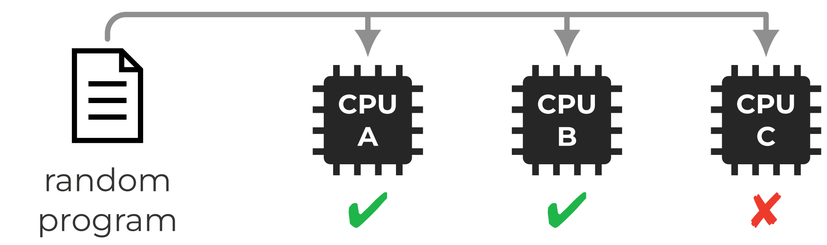
RISC-V®

open standard · no license fees · extensible

China: national policy **EU**: € 240 M programme

BUT closed chips

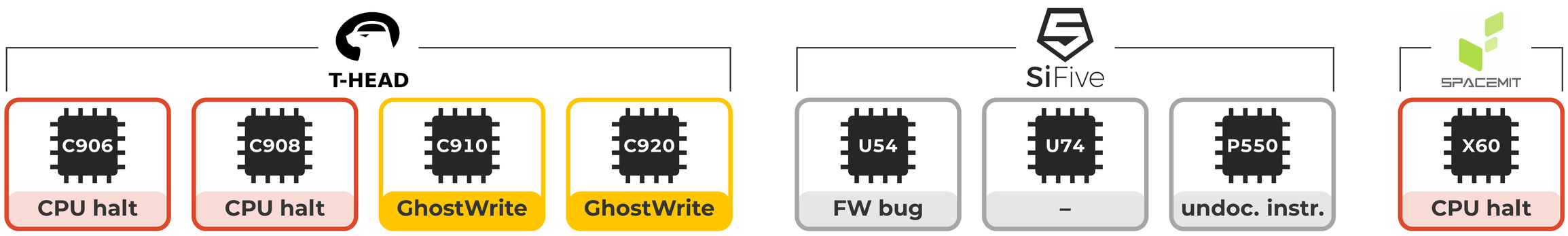
Let the Chips Check Each Other



Same program → same result? If not: **bug**.

user space · real silicon · no source code

8 CPUs • 3 Vendors • 4 Vulnerabilities



Same Instruction, Different Answers

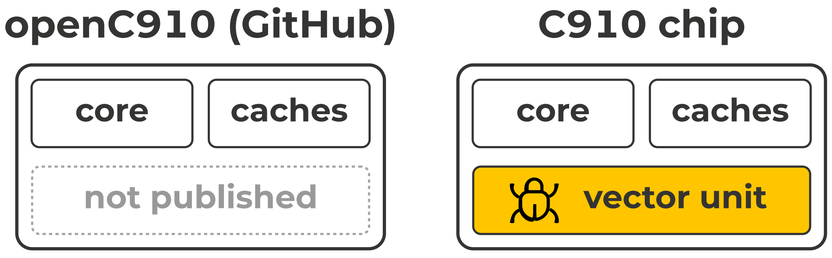
```
C906
$ ./vse1024
Segmentation fault
```

≠

```
C910
$ ./vse1024
OK
```

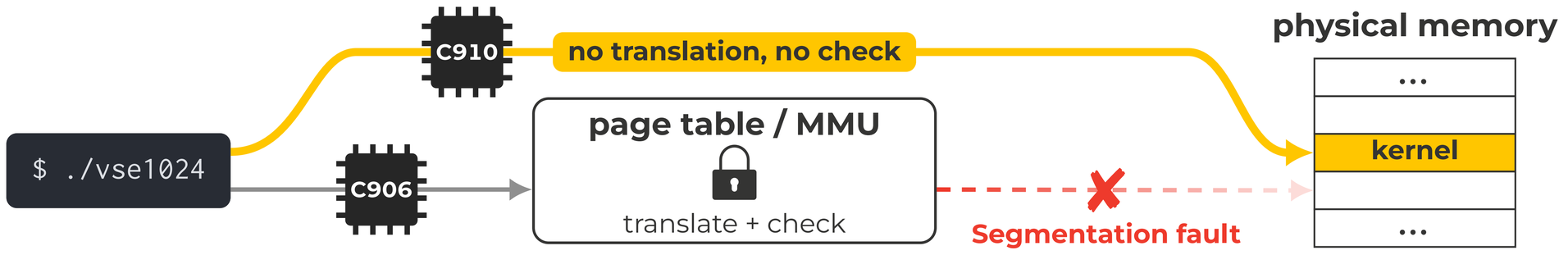
One of them is wrong.

Published Code ≠ Silicon



Simulation can't test what isn't published.

GhostWrite: Stores Skip Virtual Memory

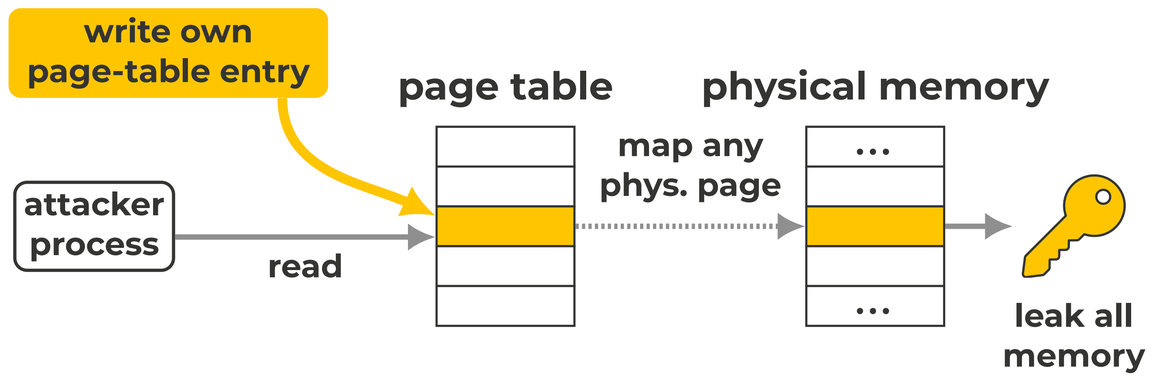


Write → Root

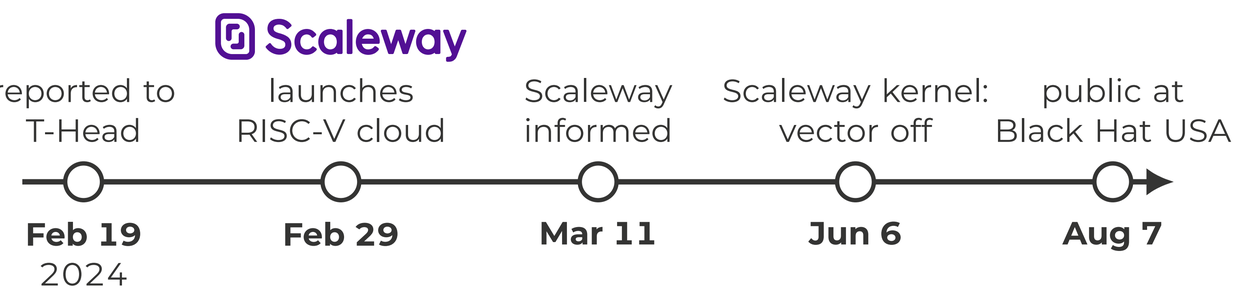


4 instructions · unprivileged · works in containers

Write → Read All Memory



Unpatchable Silicon, Mitigated in Software



no microcode → vector off: ≈ 50 % of instructions

```
C910 board
$ lscpu
Vulnerabilities:
  Gather data sampling:  Not affected
  Ghostwrite:            Mitigation: xtheadvector disabled
  L1tf:                  Not affected
  Meltdown:              Not affected
```

Linux ≥ 6.14 · try `lscpu` on your laptop

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

Artifacts Available V1.1 · Artifacts Evaluated Functional V1.1 · Results Reproduced V1.1

ghostwriteattack.com

Open source: github.com/cispa/RISCover · CVE-2024-44067