VeriCHERI: Exhaustive Security Verification of CHERI Processors

Speaker: Tobias Jauch

RISC-V Summit Europe

12. – 15.05.2025, Paris

Anna Lena Duque Antón, Johannes Müller, Philipp Schmitz,
Tobias Jauch, Alex Wezel, Lucas Deutschmann,
Mohammed R. Fadiheh, Dominik Stoffel, and Wolfgang Kunz

RPTU Rheinland-Pfälzische Technische Universität Kaiserslautern Landau

Motivation

Goal: robust and trustworthy security mechanisms

Major challenge: memory safety

Solution: Capabilities / CHERI

CHERI

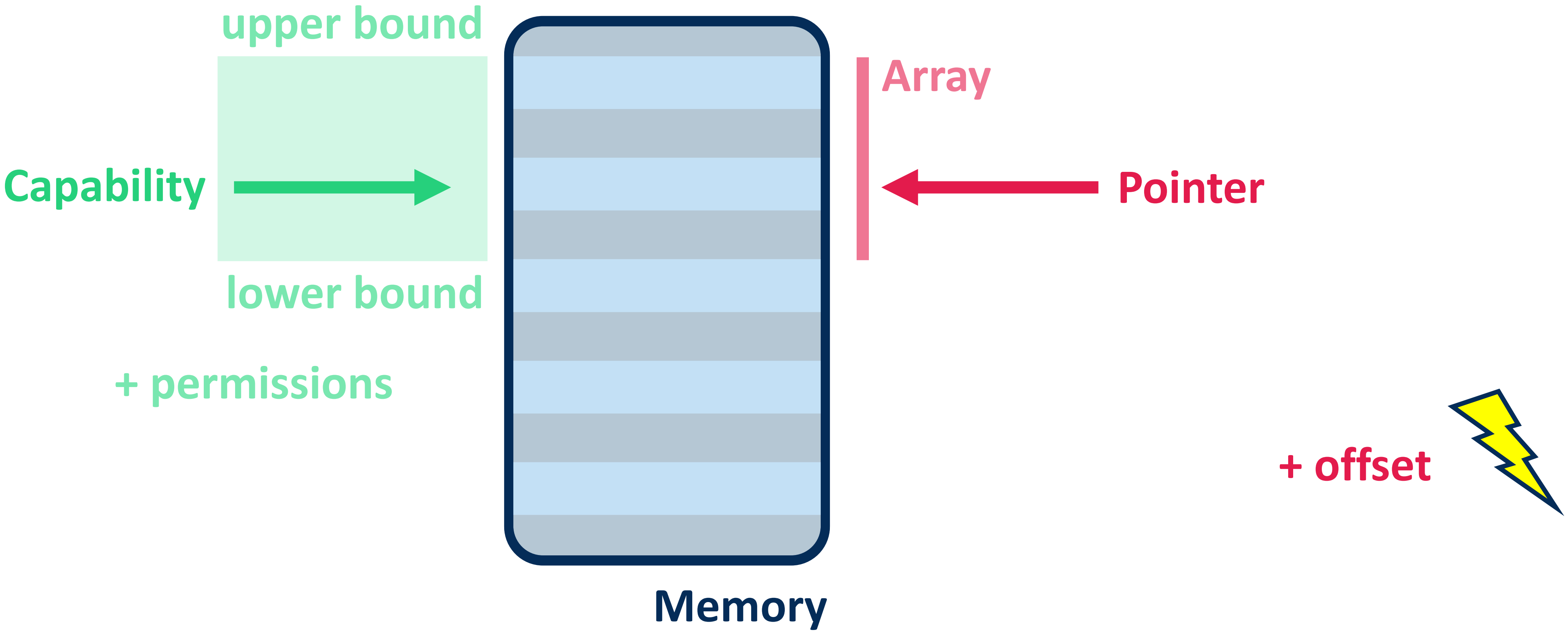
Solution: Capabilities / CHERI

Capability Hardware Enhanced RISC Instructions

Fine-grained memory protection in hardware

Gaining traction in industry

CHERI


upper bound
Capability
lower bound
+ permissions
Array
Pointer
+ offset
Memory

Motivation

Challenge:

Comprehensive security verification necessary

Motivation

Related verification approaches:

Verification based on a formal ISA model, rendering a high manual effort [Nienhuis et al., Grisenthwaite et al.]

Functional correctness proofs, automatically derived from the SAIL specification [Ploix et al.]

Motivation

Pitfalls:

Manual translation of functional security properties might not cover every aspect and corner case of the design

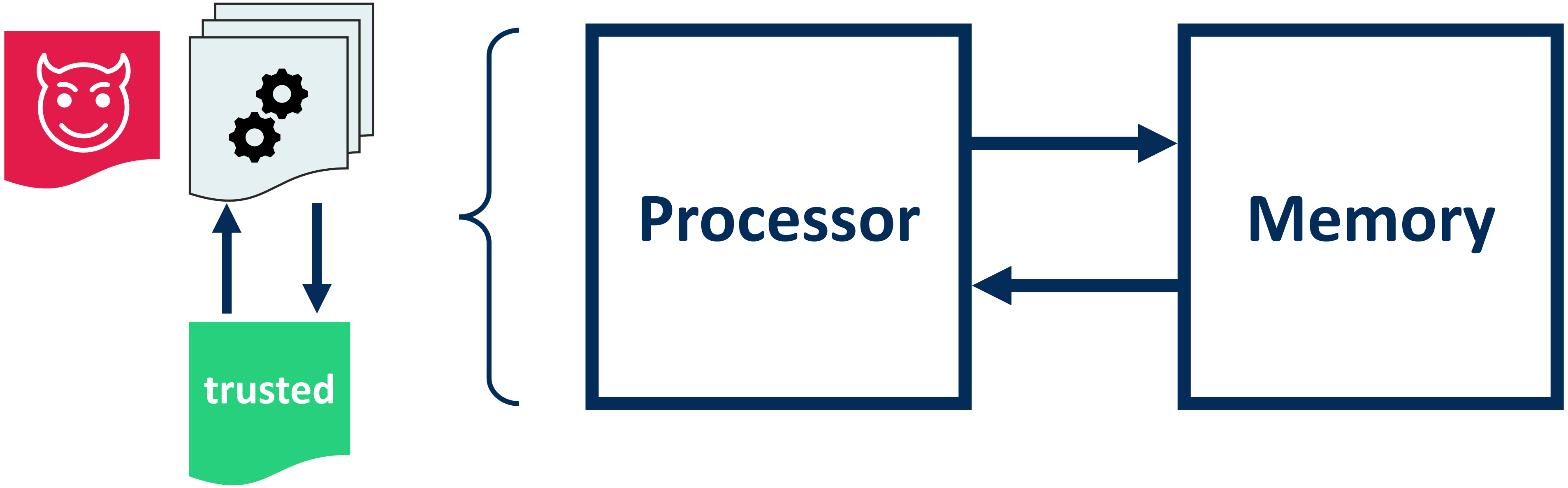
Security verification based on time-abstract ISA models misses non-functional vulnerabilities (timing side channels)

VeriCHERI

- Proves global security objectives (confidentiality, integrity)

- Uses the timing-accurate RTL impementation

Attacker Model



Security Objective

Goal:

Prove global security objectives (confidentiality, integrity)

Approach:

Model security objectives using non-interference

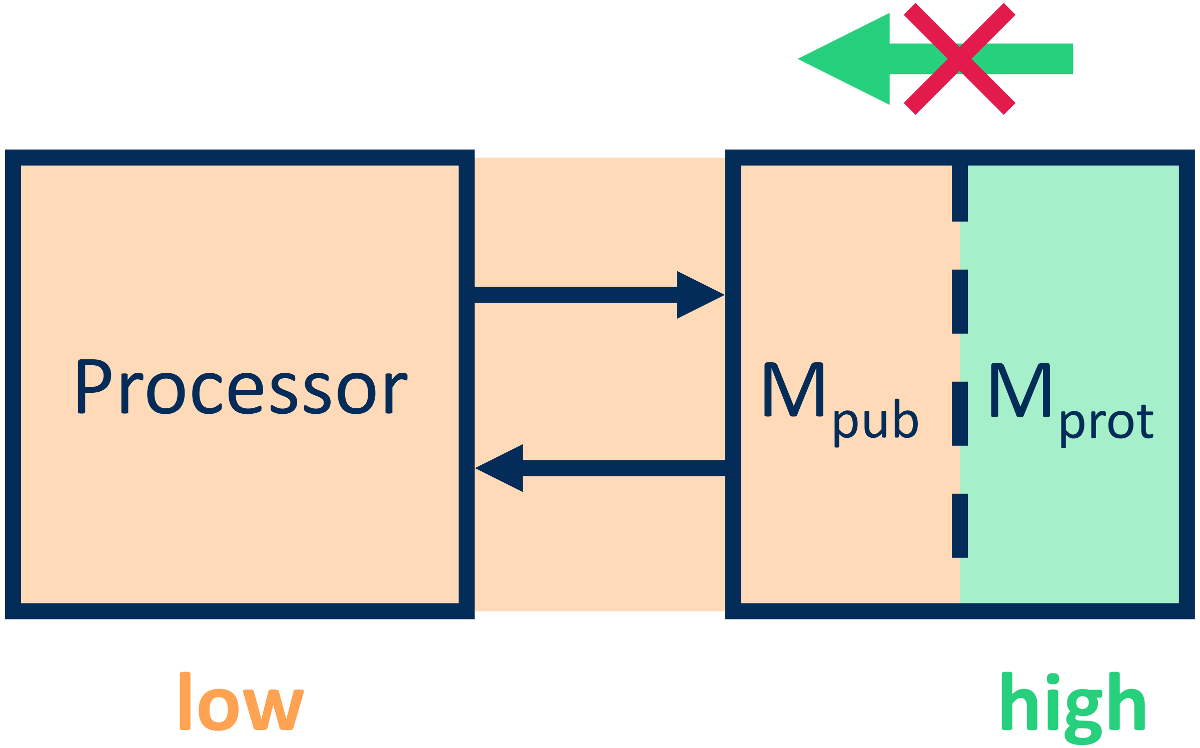
Security Objective

- Model security objectives using non-interference

  - Strong notion of security

  - Well known and widely adapted

Non-Interference



Formal Model

Confidentiality non-interference

CTL-property:

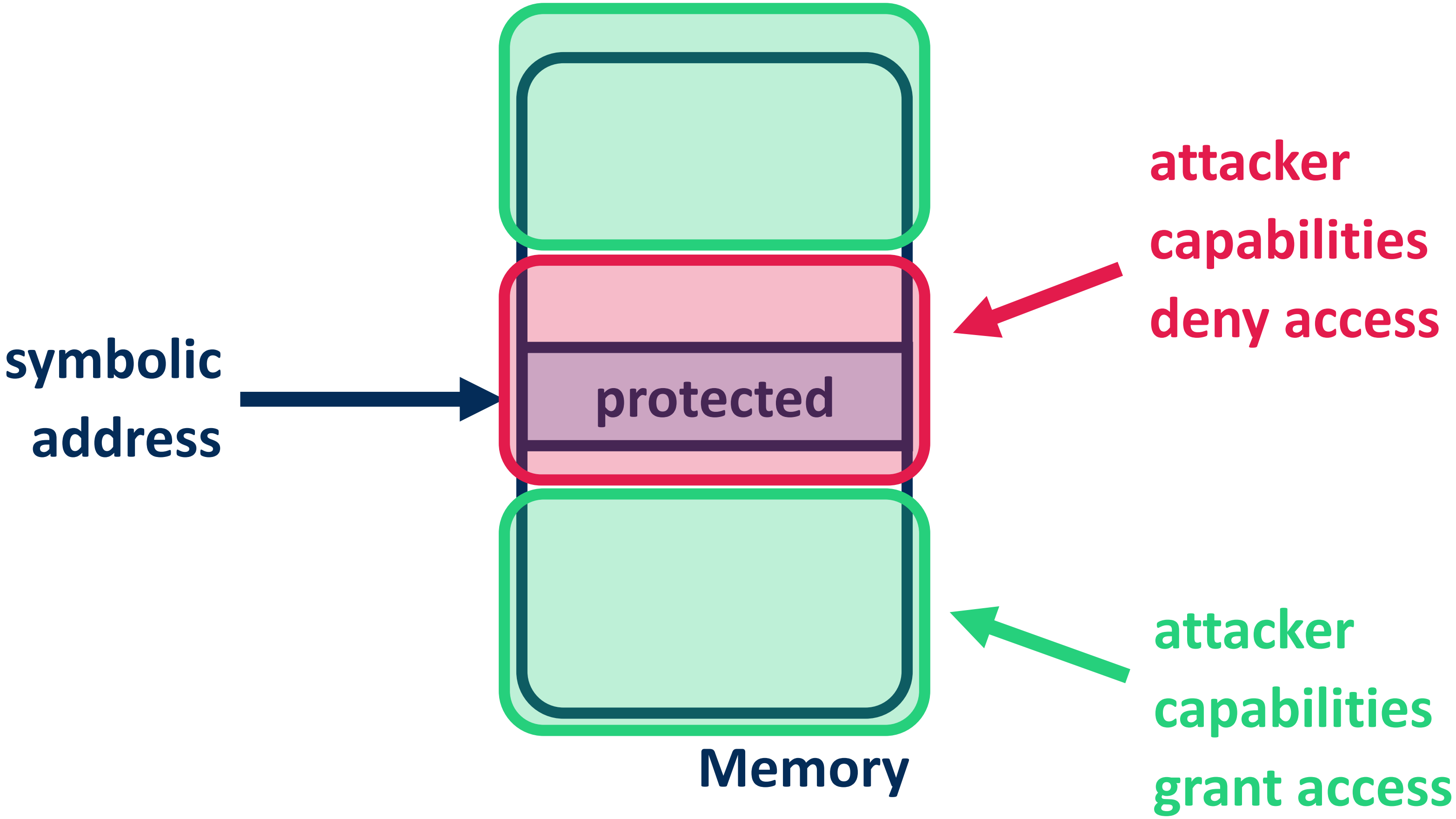
$$\mathrm{AG}(\ \$M_{pub} = \$M'_{pub} \wedge \$P = \$P' \\ \rightarrow\ \mathrm{AG}(\$M_{pub} = \$M'_{pub} \wedge \$P = \$P'\ ))$$

Integrity non-interference

CTL-property:

$$\mathrm{AG}(\ \$M_{prot} = \$M'_{prot} \\ \rightarrow\ \mathrm{AG}(\$M_{prot} = \$M'_{prot}\ )\ )$$

Formal Model



symbolic address

protected

Memory

attacker capabilities deny access

attacker capabilities grant access

Interval Properties

Confidentiality interval property:

```
t : cheri_protected(symbolic_addr)
implies
t: !read_mem ||
   mem_addr != symbolic_addr
```

Integrity interval property:

```
t : cheri_protected(symbolic_addr)
implies
t: !write_mem ||
   mem_addr != symbolic_addr
```

Interval Properties

- Properties describe the behavior in a single clock cycle

Scalable proofs

Cover every possible compartmentalization and program

Interval Properties

? What if the property fails?

Confidentiality property is a sufficient, but not a necessary condition for security

Protected data could propagate to internal buffers that are not attacker visible, without causing a leakage

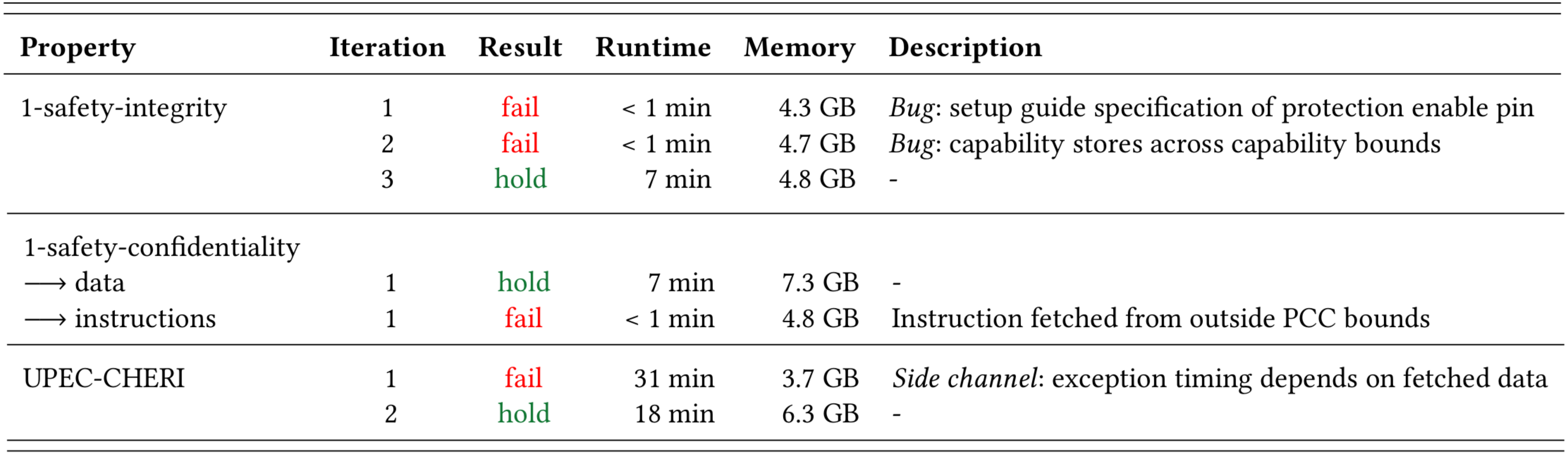
UPEC-CHERI

? What if the property fails?

We define a less conservative 2-safety property for confidentiality to cover such scenarios

Reformulation of UPEC [Fadiheh et al.] to match our CHERI-specific threat model

Case Study: CHERIoT-IBEX Processor



Property	Iteration	Result	Runtime	Memory	Description
1-safety-integrity	1	fail	< 1 min	4.3 GB	*Bug*: setup guide specification of protection enable pin
	2	fail	< 1 min	4.7 GB	*Bug*: capability stores across capability bounds
	3	hold	7 min	4.8 GB	-
1-safety-confidentiality					
⟶ data	1	hold	7 min	7.3 GB	-
⟶ instructions	1	fail	< 1 min	4.8 GB	Instruction fetched from outside PCC bounds
UPEC-CHERI	1	fail	31 min	3.7 GB	*Side channel*: exception timing depends on fetched data
	2	hold	18 min	6.3 GB	-

Case Study: CHERIoT-IBEX Processor

VeriCHERI detected a potential Transient Execution Attack

Branch to address outside PCC bounds

Exception raised, but delayed depending on two fetched bits

Performance counter changes based on the two bits

Case Study: CHERIoT-IBEX Processor

VeriCHERI detected a potential Transient Execution Attack

By measuring the execution time, an attacker can probe two bits of an arbitrary protected address

Confirmed and fixed by CHERIoT development team

Conclusion

- VeriCHERI detected several new security issues
- Scalable, iterative verification flow
- Symbolic verification IP for CHERIoT can be reused for similar designs

Thank you for your attention!

Contact me at:
tobias.jauch@rptu.de

VeriCHERI at ICCAD‘24

CHERIoT blogpost on detected vulnerability

This work was supported partly by **BMBF** Scale4Edge (16ME0122K-16ME0140+16ME0465), by **Intel** Corp., Scalable Assurance Program, by **Siemens EDA** and by **DFG** SPP NanoSecurity (KU1051/11-2). We thank the CHERIoT Ibex development team for their valuable feedback.

Appendix