Formally Verified Security @ MPI-SP

1. Security Goal

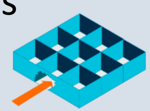
2. Enforcement

3. Formal Validation

- Cătălin Hrițcu (Faculty)
- Cezar Andrici (PhD)
- Jonathan Baumann (PhD)
- Yonghyun Kim (PostDoc)
- Julay L.-Brooks (Intern)
- Jérémy Thibault (visitor, ex-PhD)
- Rob Blanco (visitor, ex-PostDoc)

Secure compilation of compartmentalized C code

1. **Restricting scope of UB** to compromised compartments
2. **CompCert** variant to **CHERI RISC-V** capability machine
3. **Scalable machine-checked proofs in Rocq**



[Jérémy et al, CCS'18, CSF'19, ESOP'20, CSF'22, CCS'24, ITP'25]

Secure compilation of verified F* code

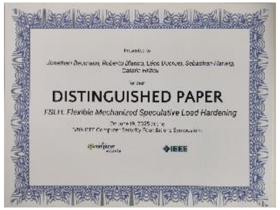
...

[Cezar et al, TYPES'22, HOPE'22, POPL'24, ICFP'25]

FS-CASA: Formally Secure Compilation Against Spectre Attacks

(collaboration with Yuval and Tim)

1. Relative security



Presented to

Jonathan Baumann, Roberto Blanco, Léon Ducruet, Sebastian Harwig, Cătălin Hrițcu

for their

DISTINGUISHED PAPER

FSLH: Flexible Mechanized Speculative Load Hardening

On June 19, 2025 at the
38th IEEE Computer Security Foundations Symposium

- compiled program doesn't leak speculatively more than what (arbitrary!) source program leaks sequentially

2. Building on FSLH: Flexible Speculative Load Hardening [Jonathan et al, CSF'25]

- Extending this to all main Spectre variants
- Want to implement this defense in LLVM

3. Testing and proving relative security

- Building new Property-Based Testing framework for LLVM and x86 (HW/SW contracts)
- Constructing machine-checked proofs in Rocq for simplified models