

Formally Verified Security, Cătălin Hrițcu

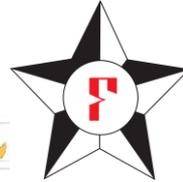
1. Security Goal



2. Enforcement



3. Formal Validation



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



Formally Verified Security, Cătălin Hrițcu

1. Security Goal 

2. Enforcement 

3. Formal Validation 
 

Secure compilation against Spectre side-channel attacks

1. **Relative security:** speculation doesn't cause extra leaks
2. **Flexible Speculative Load Hardening (SLH), Intel CET, ...**
3.  **ROCQ** proofs in simplified settings
3. **Property-based testing LLVM SLH against x86 HW-SW contract**



Formally Verified Security, Cătălin Hrițcu

1. Security Goal 

2. Enforcement 

3. Formal Validation 
 



F* proof-oriented programming language

- Secure compilation of verified F* code, proved using  and  Claude
- Dijkstra monads and incorrectness logic
- Dijkstra monads in Lean 