Formally Verified Security

1. Security Goal 

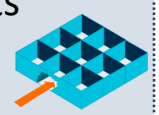
2. Enforcement 

3. Formal Proofs 

Group:

- Cătălin Hriţcu (Faculty)
- Cezar Andrici (PhD)
- Jérémy Thibault (PhD)
- Yonghyun Kim (PostDoc)
- Jonathan Baumann (ENS intern)
- Basile Schlosser (ENS intern)
- Rob Blanco (visitor, ex-PostDoc)

Secure compilation of compartmentalized C code (poster)

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

1. **Very strong guarantee**, stronger than full abstraction 
2. **Reference monitoring** and **higher-order contracts**
3. **Machine-checked proofs in F***

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

Secure compilation against Spectre side-channel attacks

- **Flexible Mechanized Speculative Load Hardening (SLH)**
  [Jonathan et al, CSF'25]
- Property-based testing **LLVM SLH** against **x86 HW-SW contract**