Proving critical systems correct: PKVM

Formal models
- of the ISA (Instruction Set Architecture)
- of the OS Interface

Proofs
- No bypassing via hardware
- Use the ISA correctly
- Provide the correct interface
- Can’t crash (segfault)
- Provide a proper separation

Thibaut Pérami