PACStack: An Authenticated Call Stack

Can we build a provably secure authenticated call stack using Pointer Authentication?

The setting:
- ARMv8.3 can compute tweakable MACs over pointers (“PACs”)
- Main goal: reverse control-flow integrity

The problem:
- Attacker can copy and reuse PACs

Approach:
- Use chained PACs to authenticate the entire call stack

Status:
- Implementation in LLVM
- Overhead: ~3% (SPEC CPU on EC2)
- Proof of security

auth₀ = H_K(ret₀, 0)
auth₁ = H_K(ret₁, auth₀)
...
authᵢ = H_K(retᵢ, authᵢ₋₁)
...
authₙ = H_K(retₙ, authₙ₋₁)

Accepted to USENIX Security 2021: https://pacstack.github.io/

Joint work with Huawei