Joint work with Huawei

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:

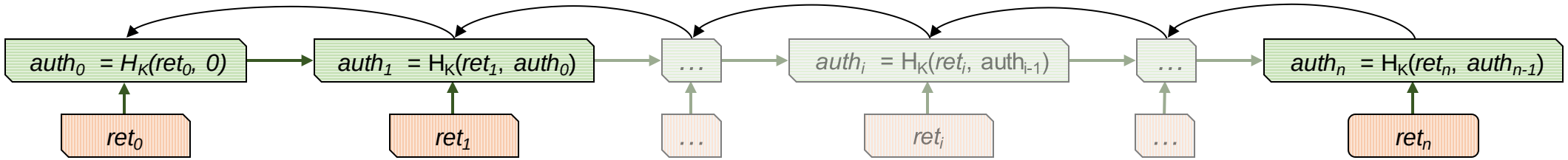
- Attacker can copy and reuse PACs

Approach:

- Use chained PACs to authenticate the entire call stack

Status:

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



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