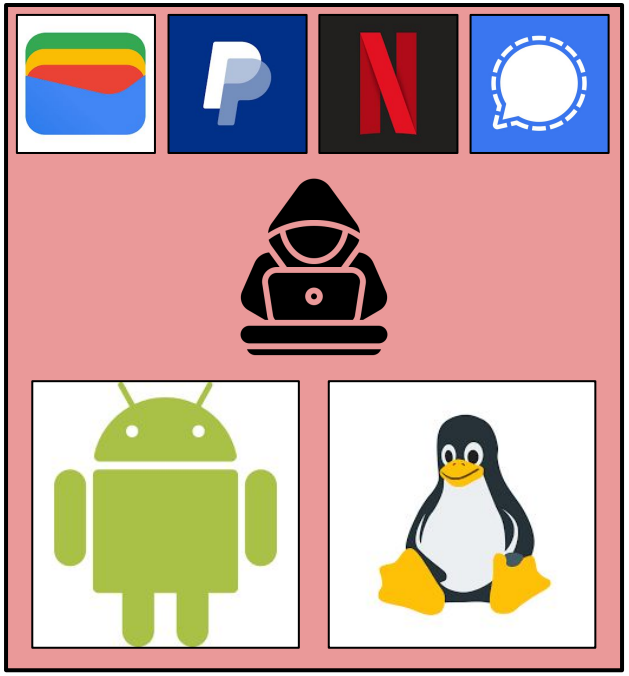
EL3XIR: Fuzzing COTS Secure Monitors

Christian Lindenmeier, Mathias Payer, Marcel Busch

christian.lindenmeier@fau.de
{marcel.busch, mathias.payer}@epfl.ch


TEEs on COTS ARMv8-A Devices

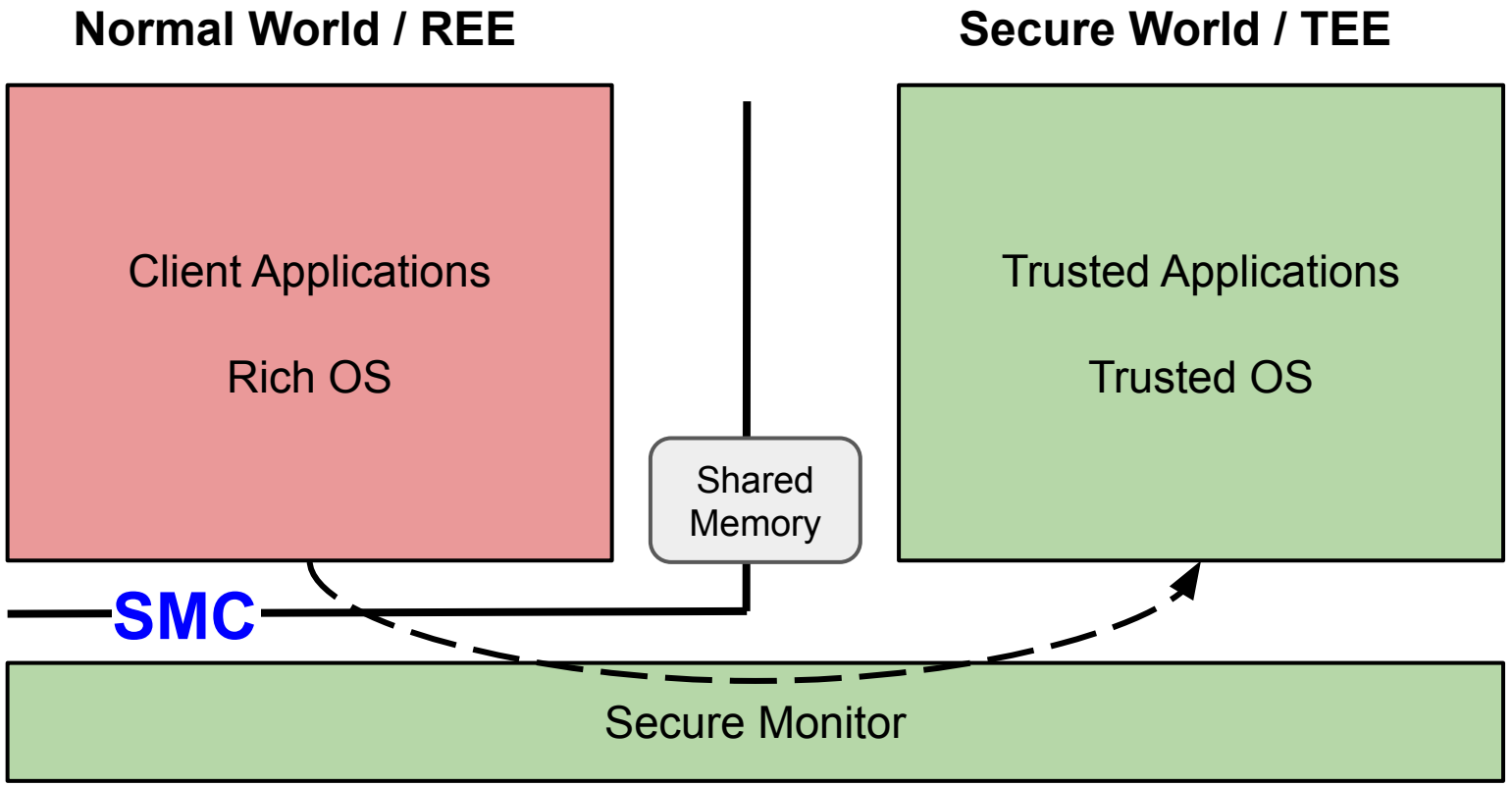


Rich Execution Environment (REE)

Trusted Execution Environment (TEE)

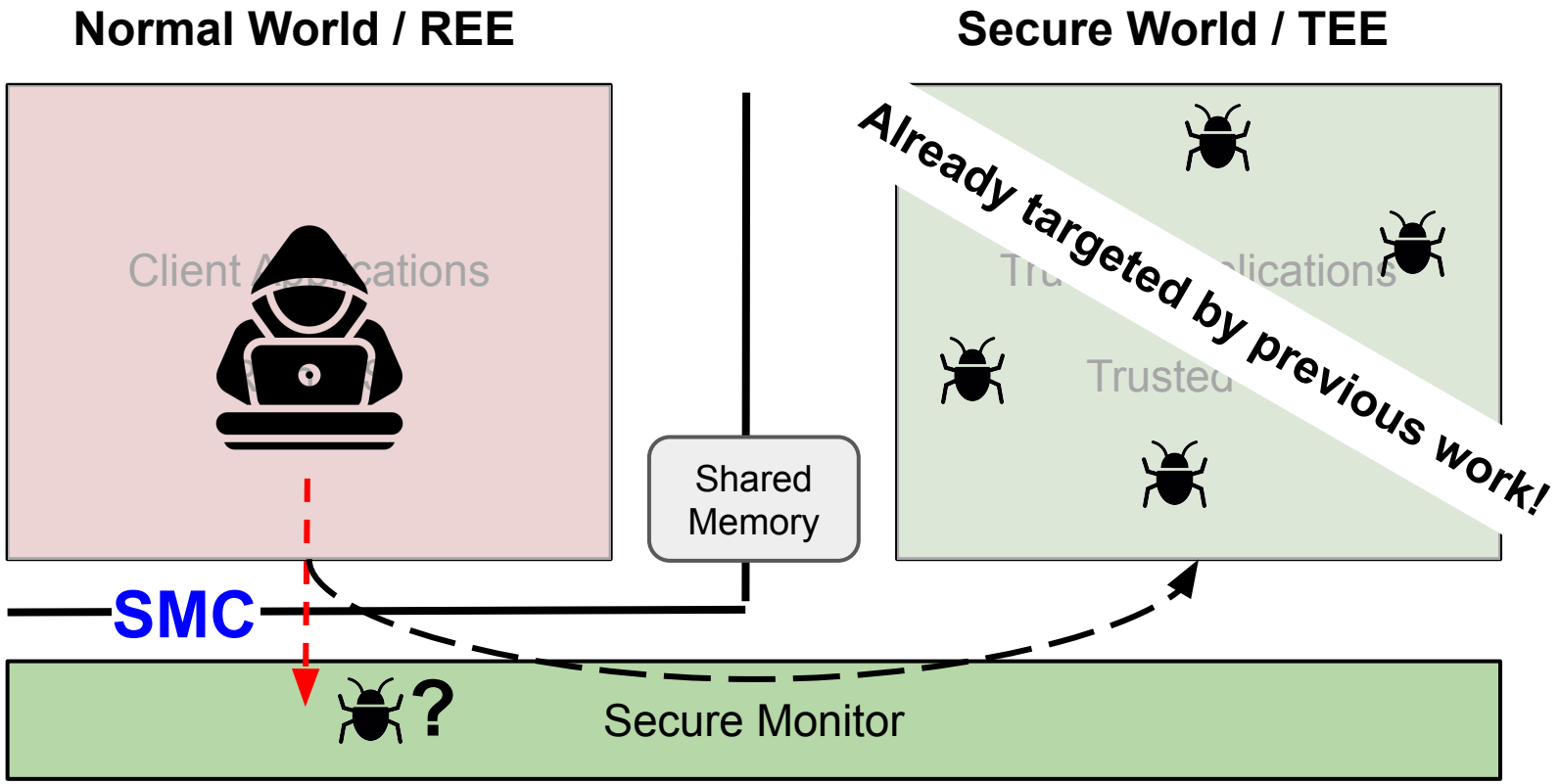
ARMv8-A TrustZone

arm TRUSTZONE



ARMv8-A TrustZone

arm TRUSTZONE



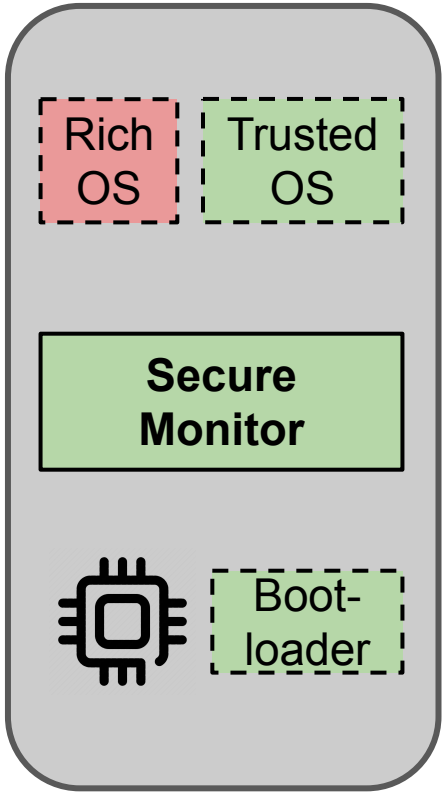
Fuzzing Secure Monitors - Challenges

C1 Limited Introspection

Rehosting: Execute firmware in an emulated environment mimicking (parts of) the original device

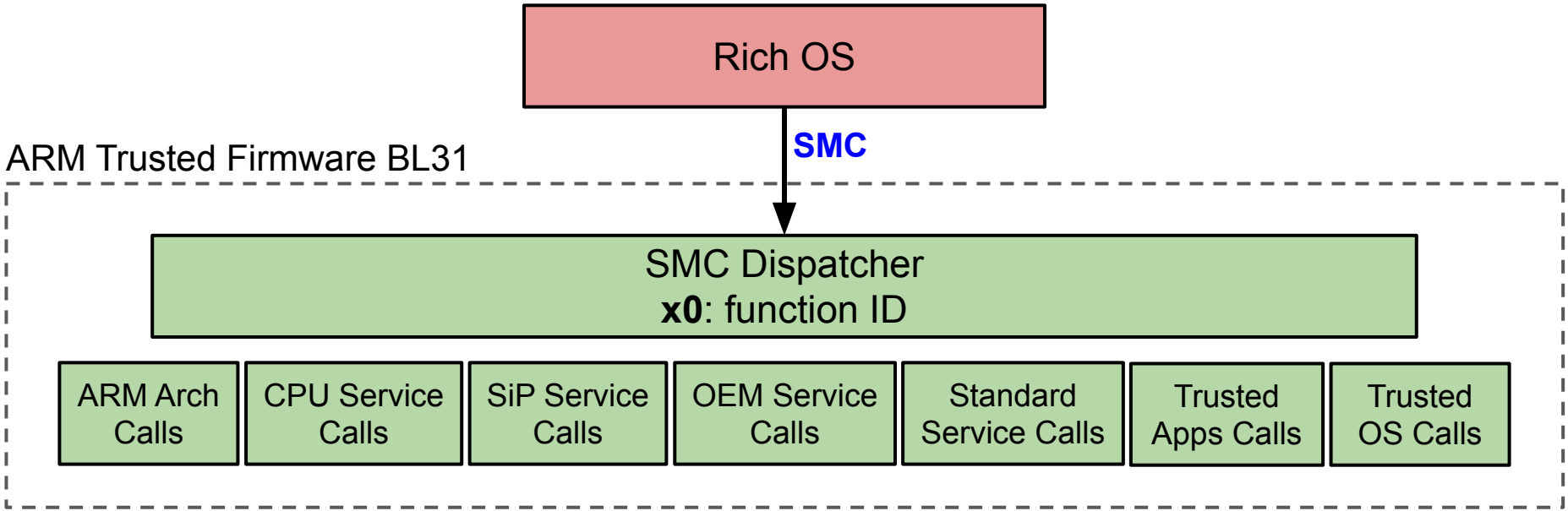
C1.1 Dependency on Software Components

C1.2 Infeasibility of Manual Peripheral Modeling



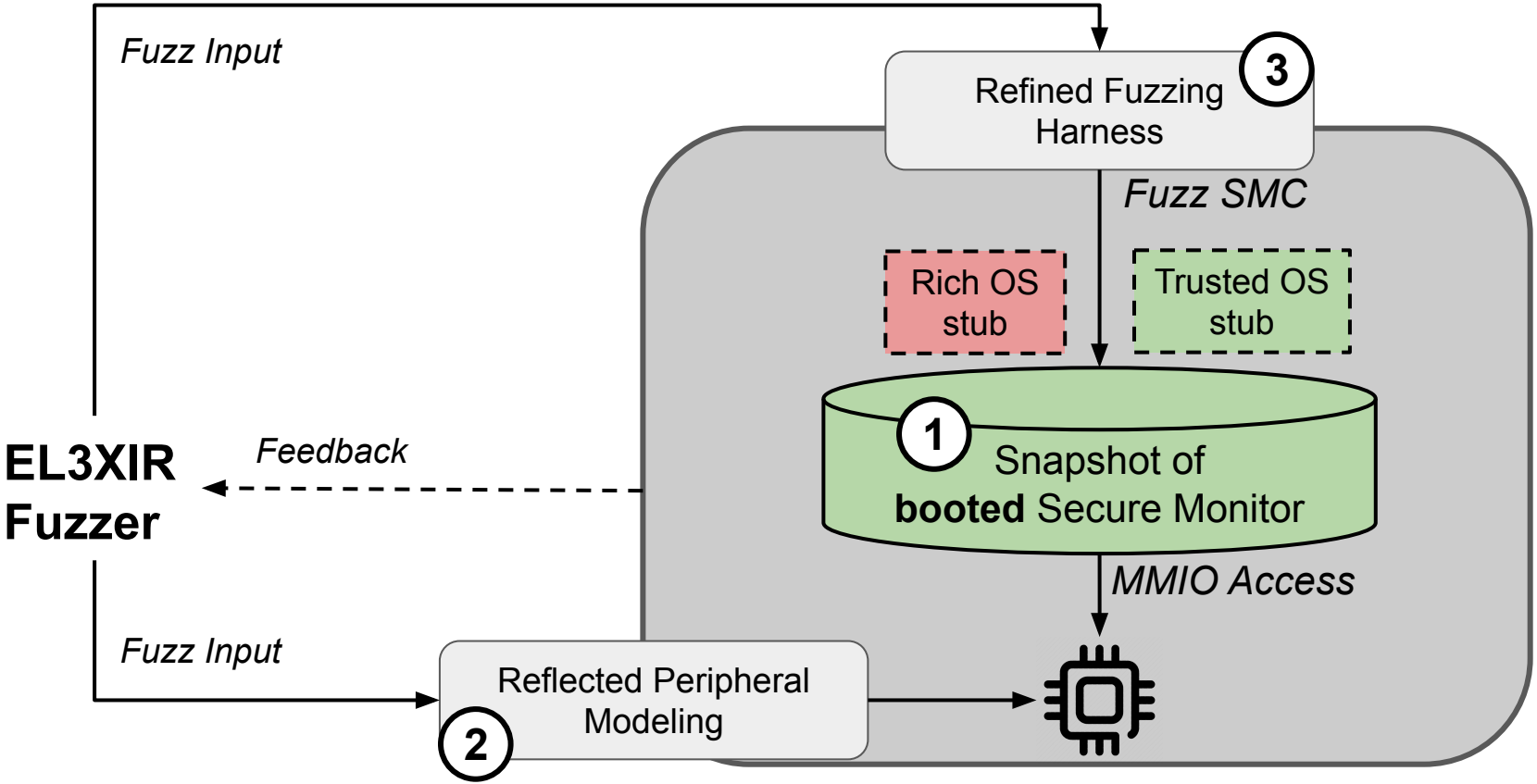
Fuzzing Secure Monitors - Challenges

C2 Complex Input Space



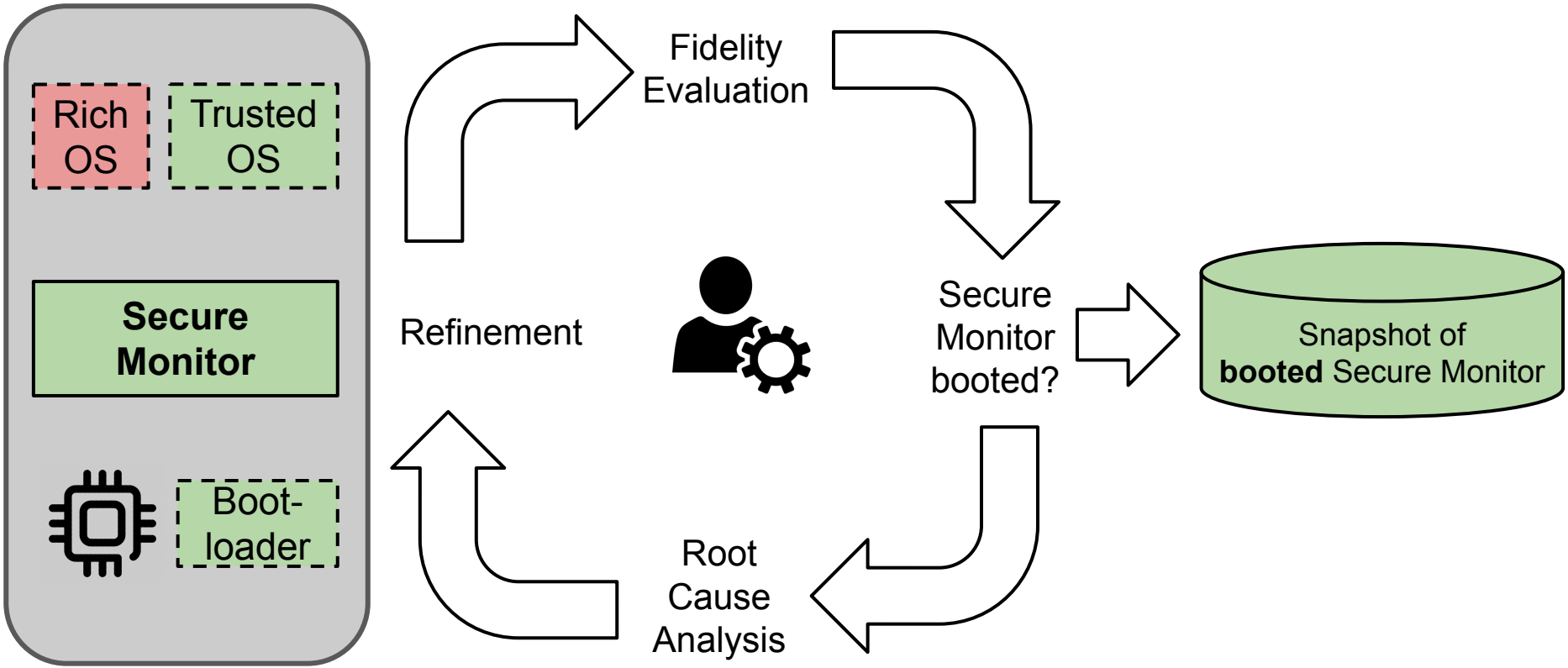
Several tens of runtime services with unique APIs…

EL3XIR's Approach - Overview



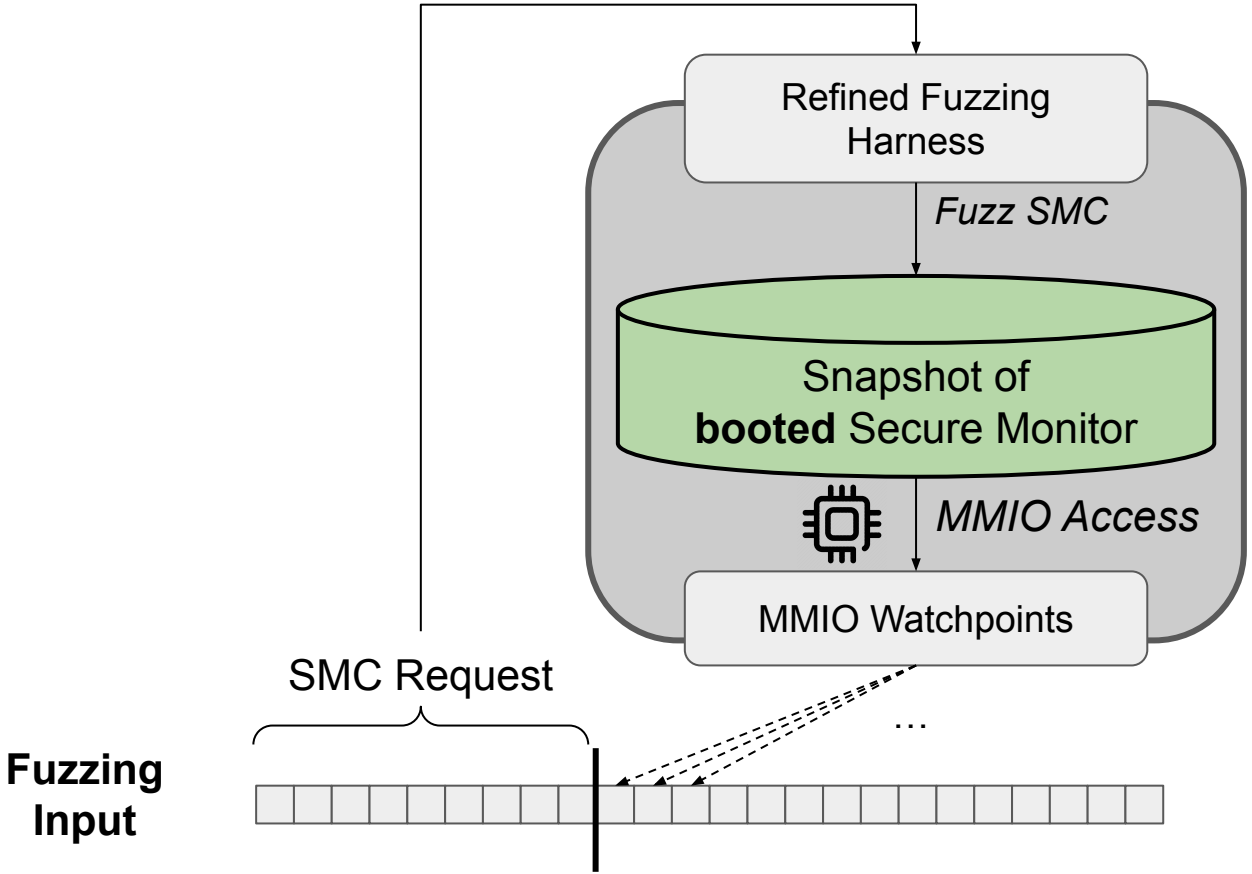
Contribution ① : Partial-Rehosting of Secure Monitors

C1.1 Dependency on Software Components



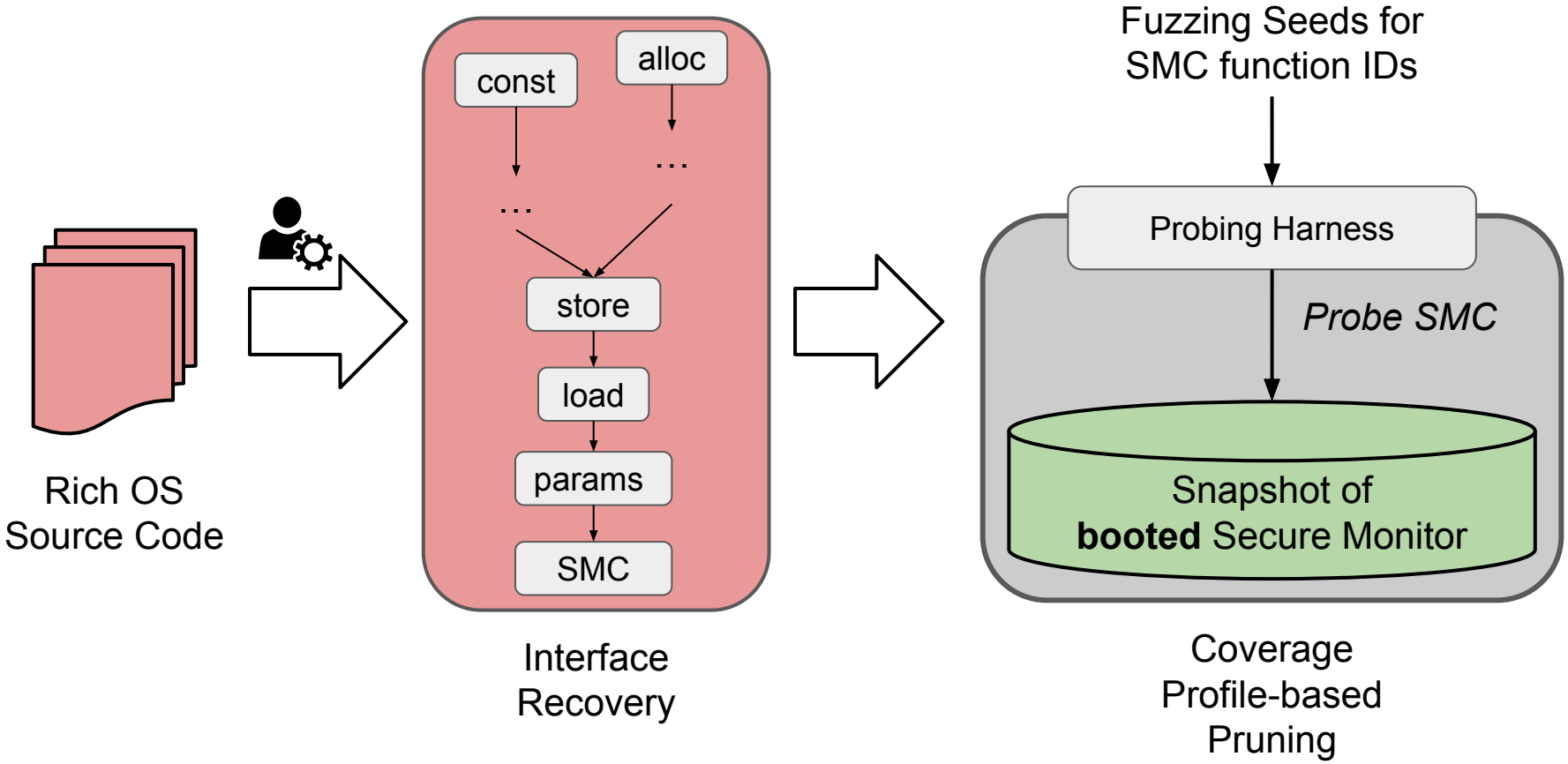
Contribution ② : Reflected Peripheral Modeling

C1.2 Infeasibility of Manual Peripheral Modeling



Contribution ③ : Harness Synthesis

C2 Complex Input Space

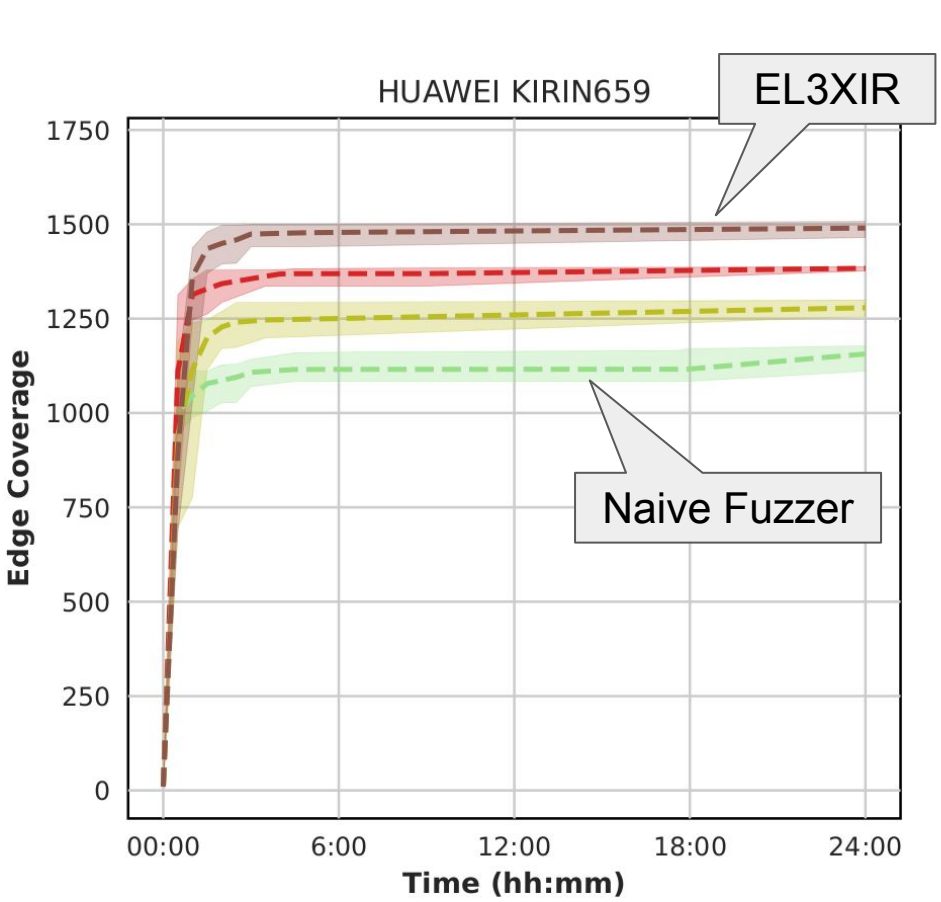


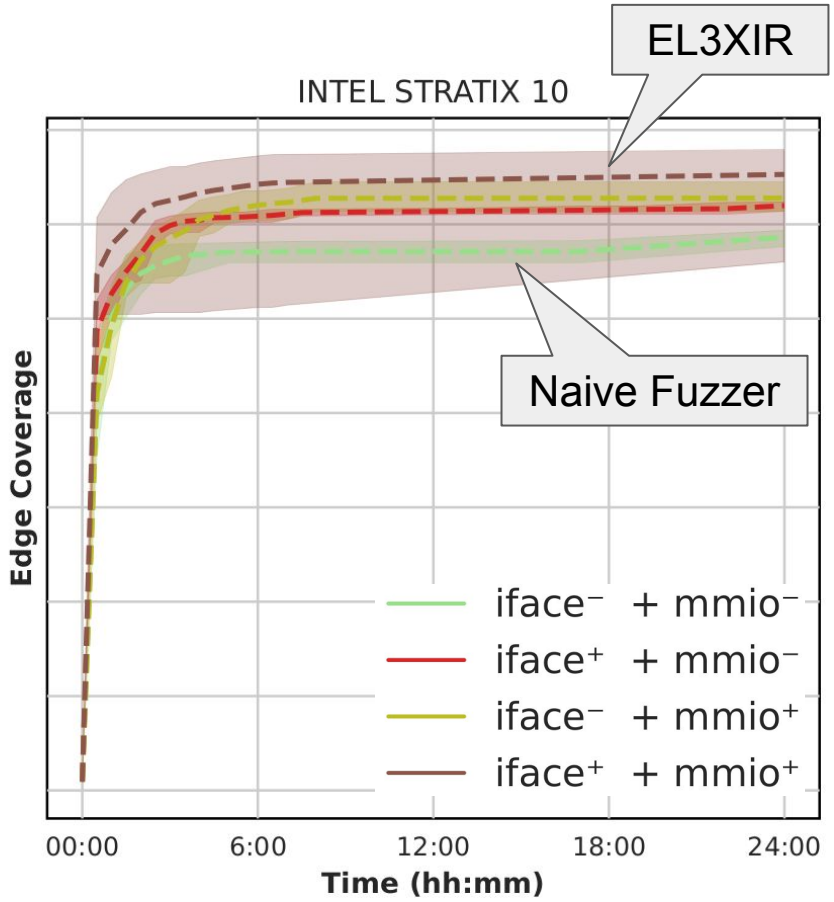
Evaluation - Bugs and CVEs

- 7 targets from 6 different vendors
  - 4 open-source, 3 closed-source
- EL3XIR triggered 34 bugs (**17** security relevant) in 5 targets
  - Naive baseline comparison triggered 19 bugs (**10** security relevant)
- Responsible disclosure resulted in 6 CVEs plus 11 confirmed bugs

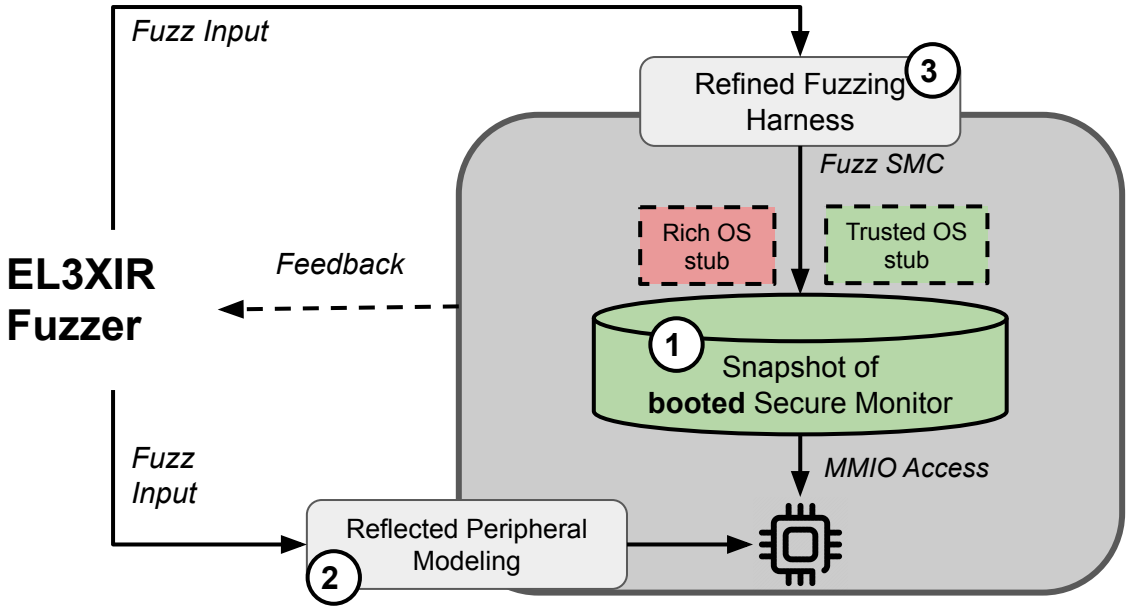
CVE-2022-38787, CVE-2023-22327 (5 different bugs), CVE-2023-49614, CVE-2024-22390, CVE-2023-31339, CVE-2023-49100

Evaluation - Coverage





EL3XIR: Fuzzing COTS Secure Monitors



github.com/HexHive/EL3XIR

- Rehosting Framework for proprietary TrustZone Firmware
- Highly automated Fuzzing Pipeline including Harness Synthesis and Peripheral Modeling
- Fuzz your own Secure Monitor

christian.lindenmeier@fau.de — 𝕏@_chli_

mathias.payer@epfl.ch — 𝕏@gannimo

marcel.busch@epfl.ch — 𝕏@0ddc0de