FAU

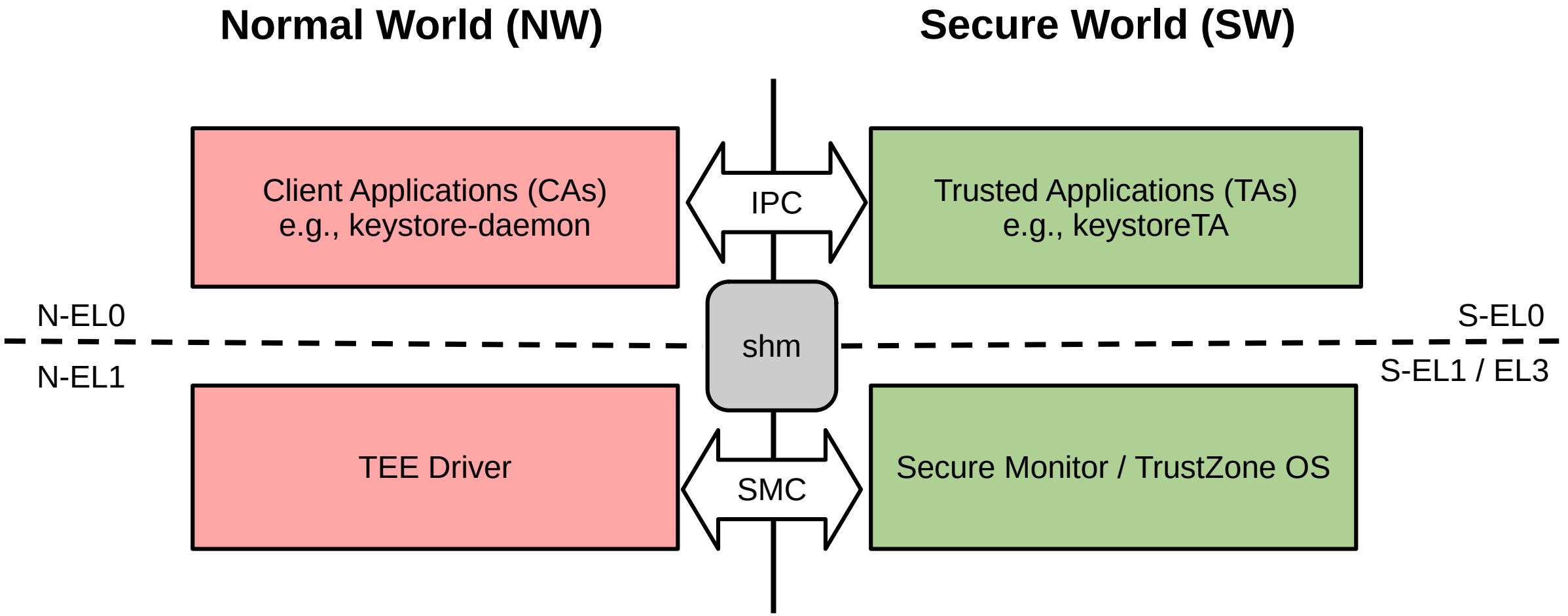
SyncEmu: Enabling Dynamic Analysis of Stateful Trusted Applications

Christian Lindenmeier[1], Matti Schulze[1], Jonas Röckl[1], Marcel Busch[2]

[1] **Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Germany**
[2] **École Polytechnique Fédérale de Lausanne (EPFL), Switzerland**

Rich Execution Environment (REE)

Trusted Execution Environment (TEE)


Normal World (NW)
Secure World (SW)
Client Applications (CAs)
e.g., keystore-daemon
IPC
Trusted Applications (TAs)
e.g., keystoreTA
N-EL0
shm
S-EL0
N-EL1
S-EL1 / EL3
TEE Driver
SMC
Secure Monitor / TrustZone OS

SyncEmu: Enabling Dynamic Analysis of Stateful Trusted Applications

Motivation

- Problem: TrustZone firmware has vulnerabilities[1]

  Multiple reasons: complex attacker model, large TCB, memory unsafe languages,…

[1]Cerdeira, D., Santos, N., Fonseca, P., & Pinto, S. (2020, May). Sok: Understanding the prevailing security vulnerabilities in trustzone-assisted tee systems. In 2020 IEEE Symposium on Security and Privacy

SyncEmu: Enabling Dynamic Analysis of Stateful Trusted Applications

Motivation

- Problem: TrustZone firmware has vulnerabilities[1]

  Multiple reasons: complex attacker model, large TCB, memory unsafe languages,…

- Static analysis is cumbersome and limited

  Multiple reasons: closed-source binaries,...

→ **We need a way to dynamically analyze COTS TrustZone firmware**

[1]Cerdeira, D., Santos, N., Fonseca, P., & Pinto, S. (2020, May). Sok: Understanding the prevailing security vulnerabilities in trustzone-assisted tee systems. In 2020 IEEE Symposium on Security and Privacy

Access to COTS smartphones is locked down

Challenge #1 – Limited Introspection

- Locked-down nature of COTS smartphones
- No accessible debug interfaces
- TrustZone extensions prevent memory introspection

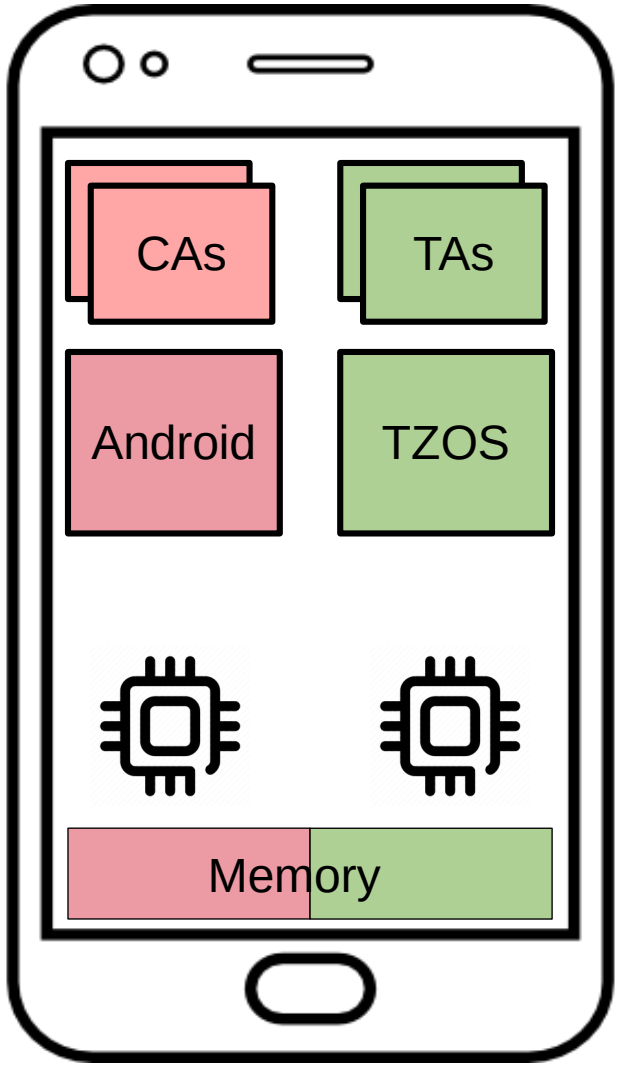
→ **On-device dynamic analysis not feasible**

- Previous work limited e.g., black-box fuzzing[2]

[2] Busch, M., Machiry, A., Spensky, C., Vigna, G., Kruegel, C., & Payer, M. (2023, May). Teezz: Fuzzing trusted applications on cots android devices. In 2023 IEEE Symposium on Security and Privacy

Challenge #1 – SyncEmu's Approach

Rehosting TrustZone OS Firmware

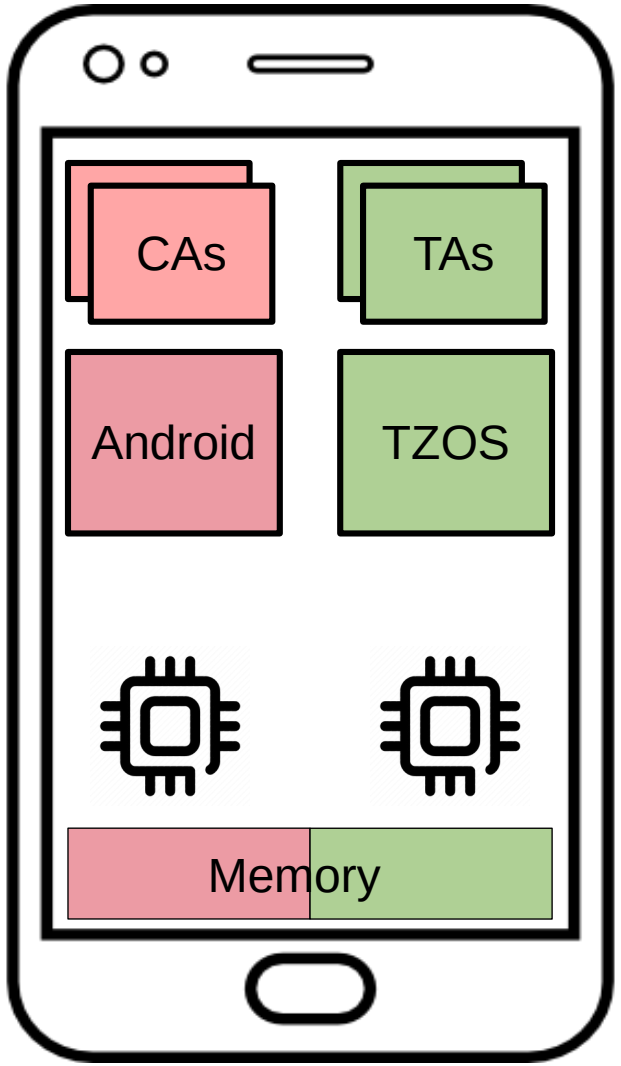


Rehosting: We execute the targeted software in an emulated environment which mimics (necessary parts of) the original device

→ Only rehost TZOS and TAs

Challenge #1 – SyncEmu's Approach

Rehosting TrustZone OS Firmware

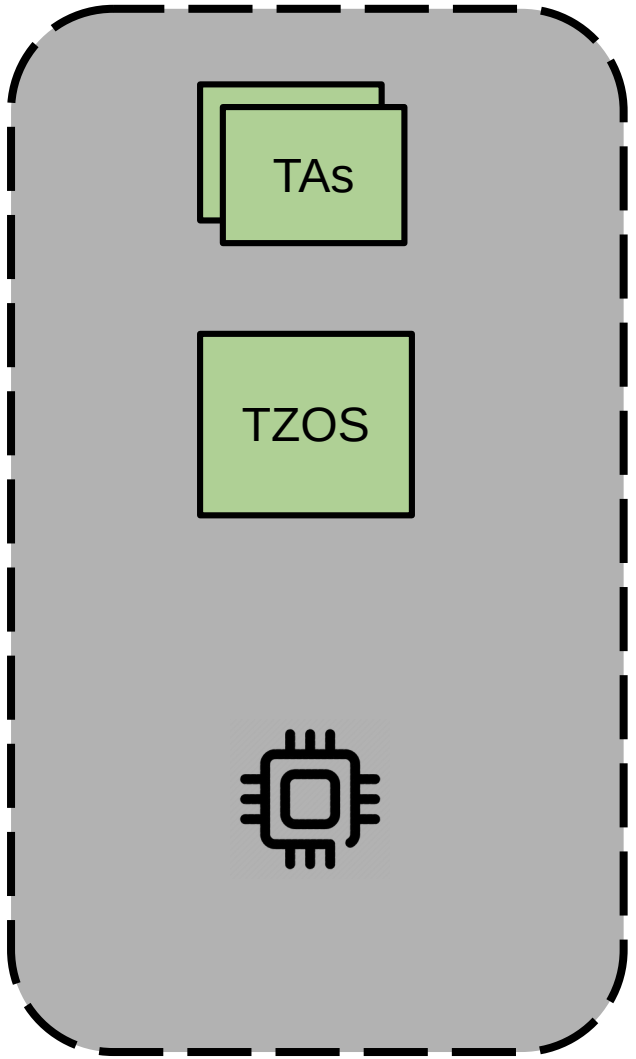


Rehosting: We execute the targeted software in an emulated environment which mimics (necessary parts of) the original device

→ Only rehost TZOS and TAs

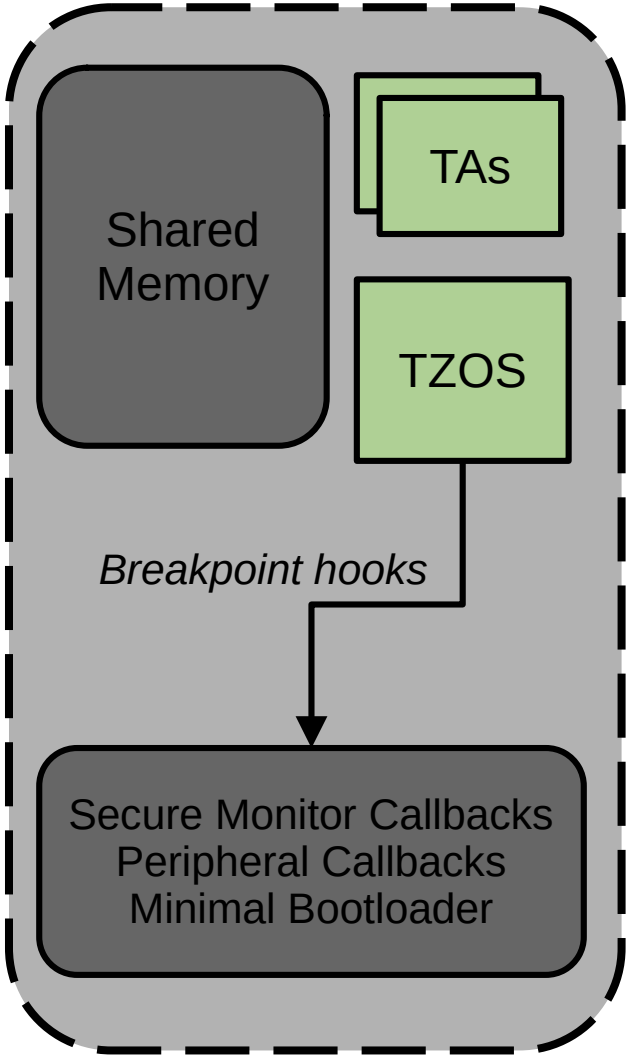
Challenges:

- Unknown physical memory map
- Missing peripherals
- Proprietary and complex hardware (fingerprint sensor, crypto cells)
- Intertwined software components



SyncEmu's Rehosting Framework

Overview

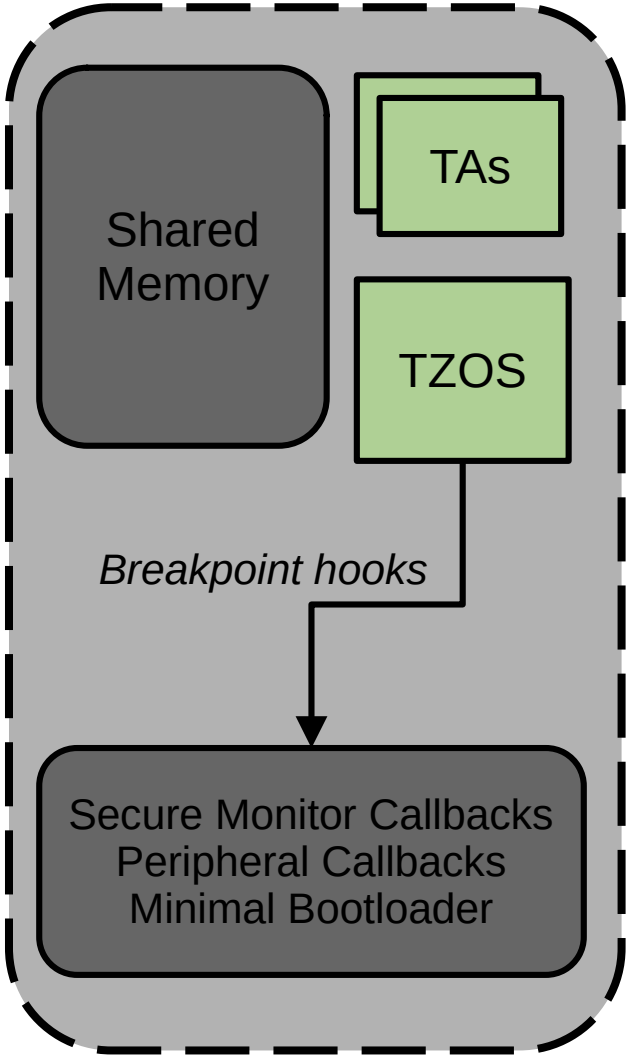


Identify main dependencies

- Bootloader Emulation
  Mimic bootloader stages
- Secure Monitor Emulation
  Handle SMCs
- Hardware Emulation
  Handle MMIO accesses

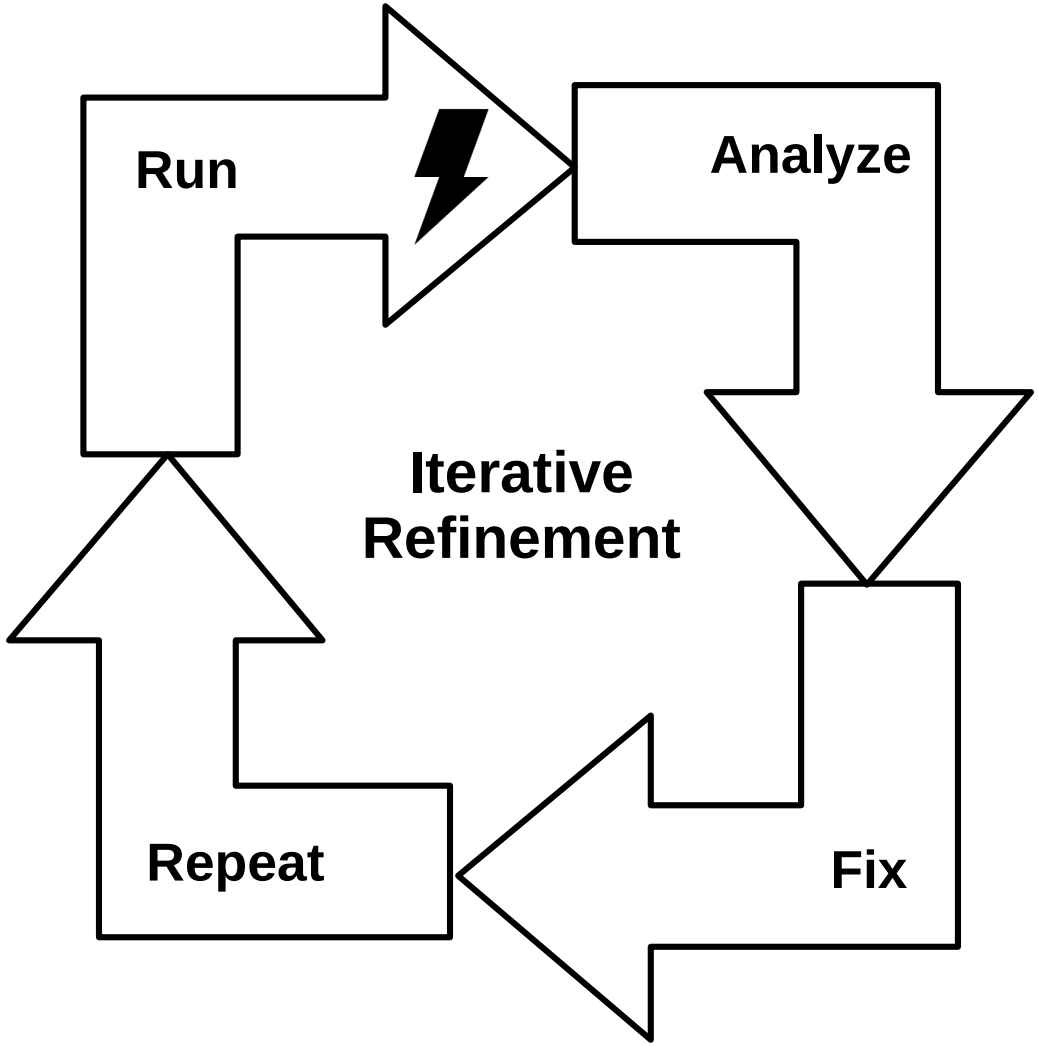
SyncEmu's Rehosting Framework

Overview



Identify main dependencies

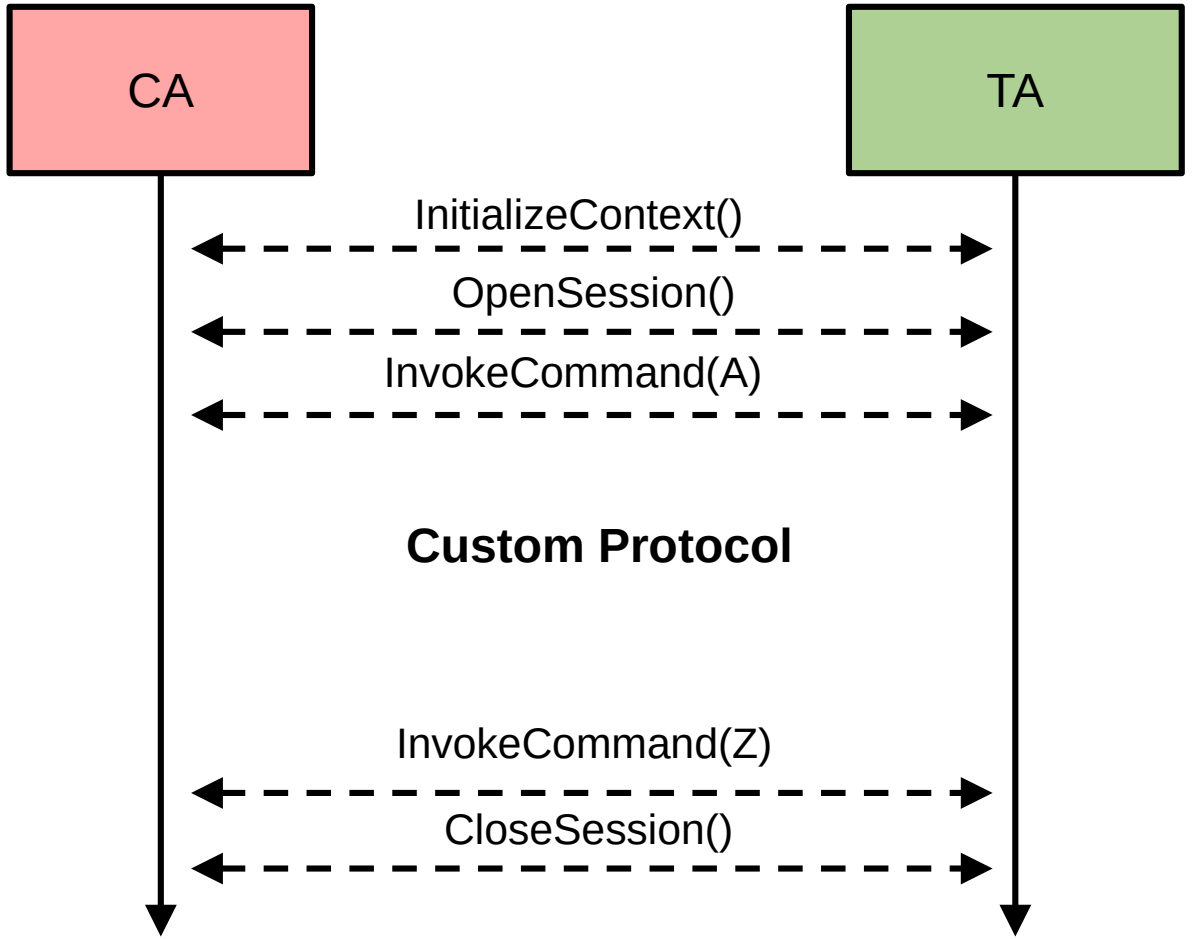
- Bootloader Emulation
  Mimic bootloader stages
- Secure Monitor Emulation
  Handle SMCs
- Hardware Emulation
  Handle MMIO accesses



Challenge #2 – Complex CA-TA Protocols

- GlobalPlatform defines interfaces for TAs
- Custom protocols depending on use case of TA
- TA execution is highly stateful
- Previous work tried emulating NW components[3]

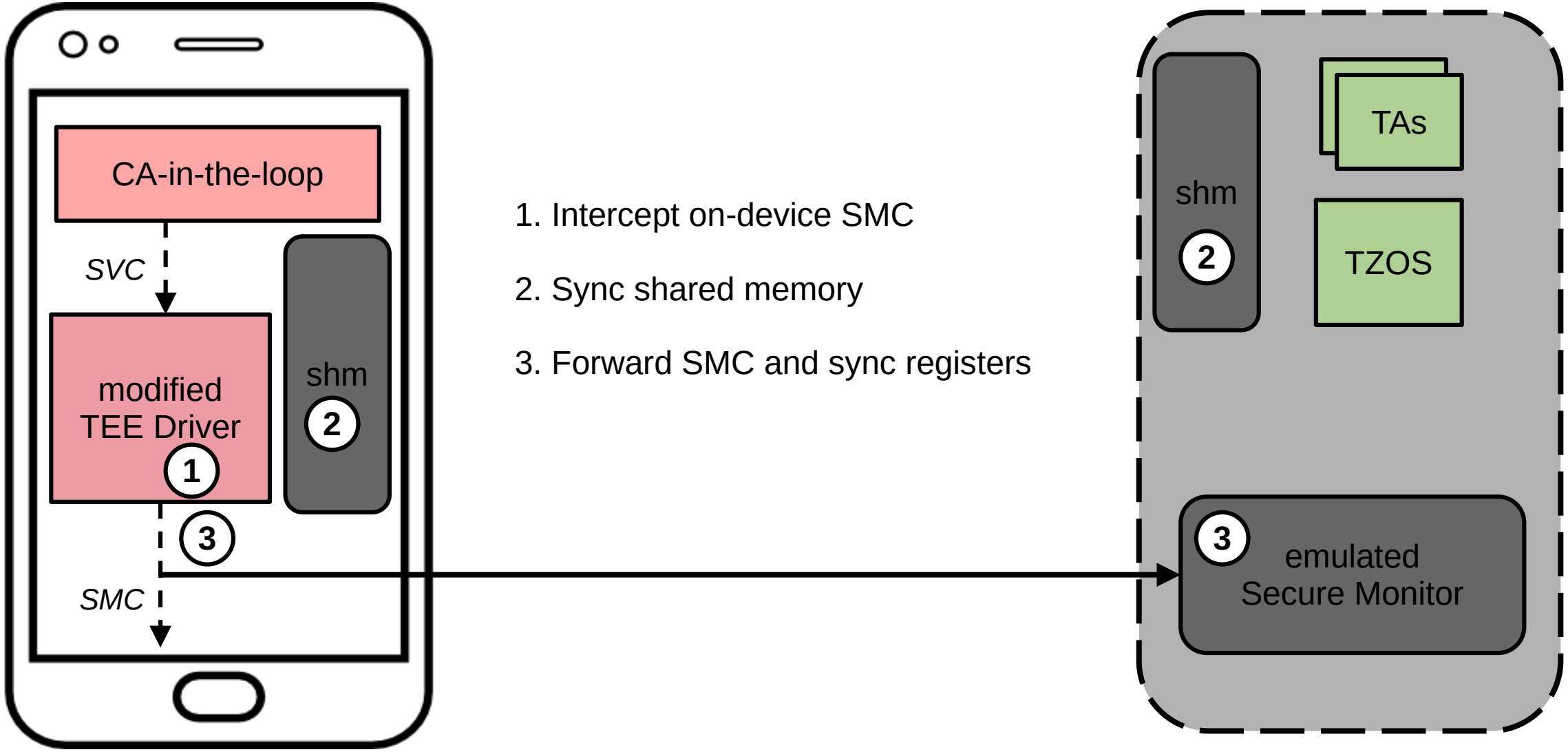
→ **Rehosting NW is not feasible**



[3]Harrison, L., Vijayakumar, H., Padhye, R., Sen, K., & Grace, M. (2020). PARTEMU: Enabling Dynamic Analysis of Real-World TrustZone Software Using Emulation. In 29th USENIX Security Symposium

SyncEmu's CA-in-the-loop Technique

Forwarding SMCs



Evaluation

Feasibility of Rehosting TZOS Implementations

Rehosting **TrustedCore** from Huawei's P9lite smartphone

- Minimal Bootloader: 19 assembly instructions
- Peripheral Callbacks: 18 emulated MMIO accesses
- Secure Monitor Callbacks: Hook at first SMC by TrustedCore and pause emulation

```
 pc=0xc0013de8: SRE_HuntByName
2024-07-06 10:23:14,721 a2scripts.tc_progress_monitor [INFO]
 pc=0x41ddffc: REET: __start_tz
2024-07-06 10:23:14,746 a2scripts.optee_secure_monitor [INFO
] SMC 0xb2000000 received, handler: _handle_return_from_tzos
_boot
TrustedCore booted!
pc=600       r0=b2000000  r1=c001fb00  r2=c001fc60  r3=2
     r4=40004     r5=50005     r6=60006     r7=70007     r8=
80008     r9=90009     r10=a000a     r11=41f82e4   r12=41f82
e8
None
christian@ThinkPad:~/Schreibtisch/PhD/syncemu$
```

```
[2000] Client connected: 127.0.0.1:54784
[2002] Client connected: 127.0.0.1:47226
[2000] TrustedCore Release Version iCOS_MAIN_2.9.0_EVA_1.6,
Nov  9 2016.18:32:24
[2000] DX_CclibInit success
[2000] invalid magic: 0x00000000
[2000] ipc: bsp_ipc_init ipc init success
[2000] invalid g_param_cfg
[2000] icc: param_cfg_init bsp_cfg_base_addr_get is NULL
[2000] icc: bsp_icc_init chan fifo init err
[2000] icc: bsp_icc_init icc init errno: 0xffffffff
[2000] Error initializing runtime service icc_driver
[2000] [TEEGlobalTask]1/2/1970 12:24:29.2999 TrustedCore Exe
cute Successfully and jump to Linux  kernel
[2000] Client disconnected: 127.0.0.1:54784
[2002] Client disconnected: 127.0.0.1:47226
```

Evaluation

CA-in-the-loop

Rehosting environments are hard to evaluate because we have not ground truth

- Approach: **Input-Output methodology**[4]
  → Compare return values of on-device TEE and rehosted TEE

[4]Fasano, A., Ballo, T., Muench, M., Leek, T., Bulekov, A., Dolan-Gavitt, B., ... & Robertson, W. (2021, May). Sok: Enabling security analyses of embedded systems via rehosting. In Proceedings of the 2021 ACM Asia conference on computer and communications security

Evaluation

CA-in-the-loop

Rehosting environments are hard to evaluate because we have not ground truth

- Approach: **Input-Output methodology**[4]
  → Compare return values of on-device TEE and rehosted TEE

- Experiment 1: OP-TEE with QEMU's machine virt
- Experiment 2: Huawei P9lite with modified TEE Driver (~300 lines C)

→ **Hardware emulation is the limiting factor**

API function	OP-TEE's aesTA	TC's keymasterTA
TEEC_InitializeContext	79 (79)	56 (56)
TEEC_OpenSession	1 (1)	56 (56)
TEEC_InvokeCommand	8 (8)	56 (0*)
TEEC_CloseSession	1 (1)	56 (56)

[4]Fasano, A., Ballo, T., Muench, M., Leek, T., Bulekov, A., Dolan-Gavitt, B., ... & Robertson, W. (2021, May). Sok: Enabling security analyses of embedded systems via rehosting. In Proceedings of the 2021 ACM Asia conference on computer and communications security

Discussion

Limitations and Future Work

Limitations:

- Physical smartphone required for CA-in-the-loop (low scalability)
- TZOS and TA binaries required (may be encrypted)
- DMA and unique hardware secrets

FAU

Limitations:

- Physical smartphone required for CA-in-the-loop (low scalability)
- TZOS and TA binaries required (may be encrypted)
- DMA and unique hardware secrets

Future Work:

- Finding strategies to emulate peripherals easier and more accurate
- Extend with other TZOS implementations
- Integrate security testing (e.g. fuzzing)

Summary

Thanks for your attention!

SyncEmu: Enabling Dynamic Analysis of Stateful Trusted Applications

Christian Lindenmeier
FAU Erlangen-Nürnberg
christian.lindenmeier@fau.de

Matti Schulze
FAU Erlangen-Nürnberg
matti.schulze@fau.de

Jonas Röckl
FAU Erlangen-Nürnberg
jonas.roeckl@fau.de

Marcel Busch
EPFL
marcel.busch@epfl.ch

- Open source rehosting framework for proprietary TrustZone images
- Showcasing CA-in-the-loop technique
- Identify future directions for research in TEE rehosting

https://github.com/syncemu/syncemu