Towards Trustworthy TEE Systems

David Cerdeira

Advisor :

Prof. Sandro Pinto

Co-Advisors:

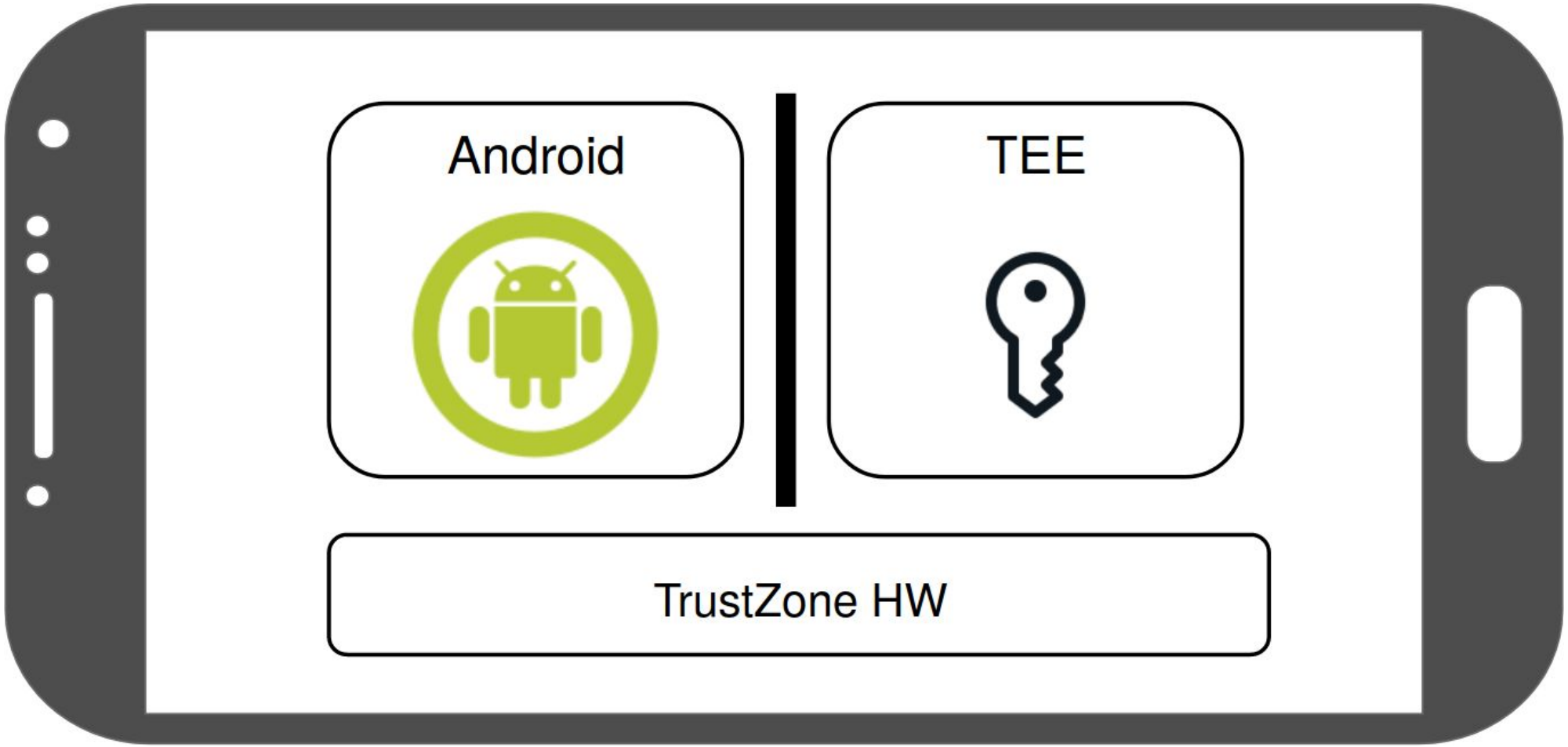
Prof. Nuno Santos & Prof. Pramod Bhatotia

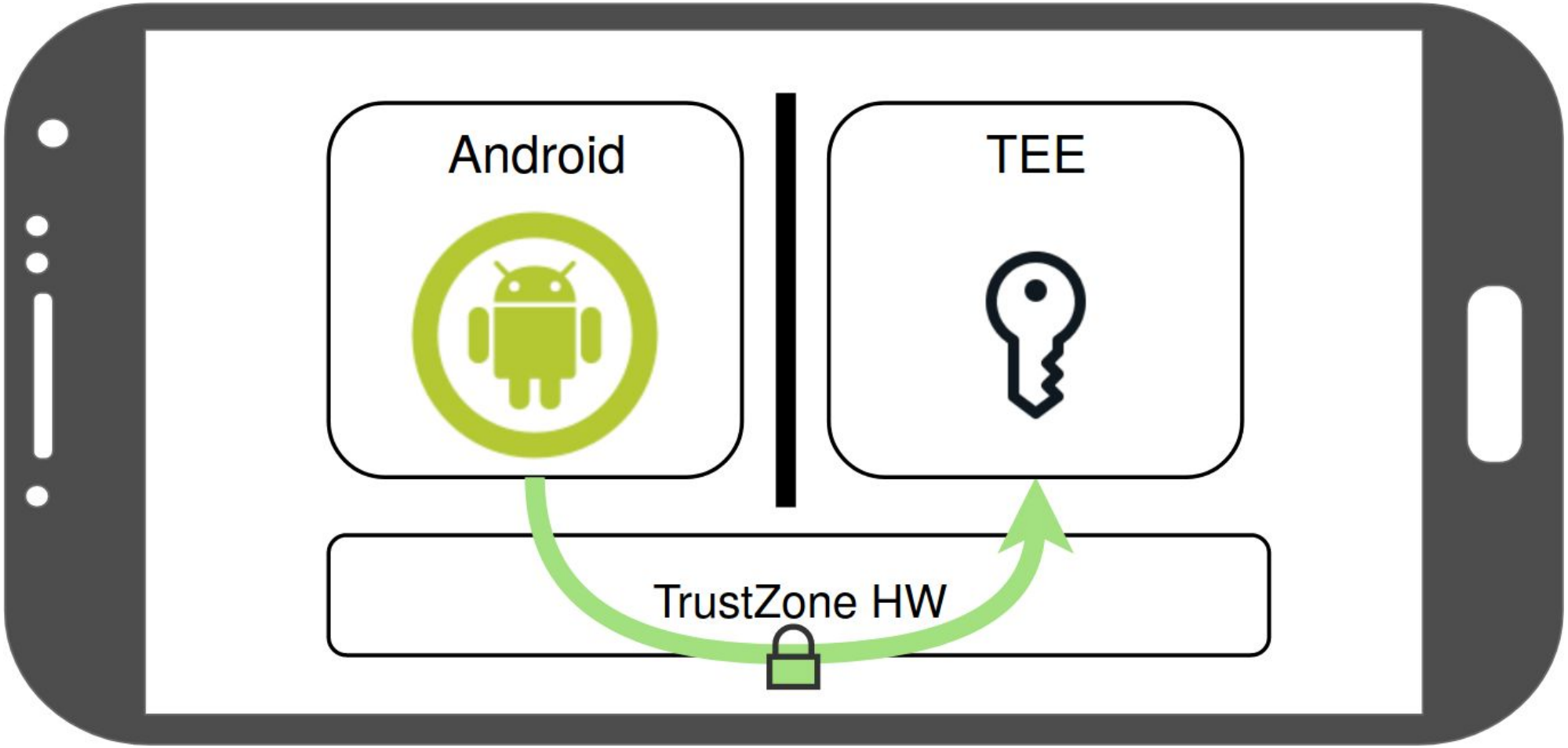
FCT Fundação para a Ciência e a Tecnologia

CENTROALGORITMI

UNIVERSIDADE DO MINHO

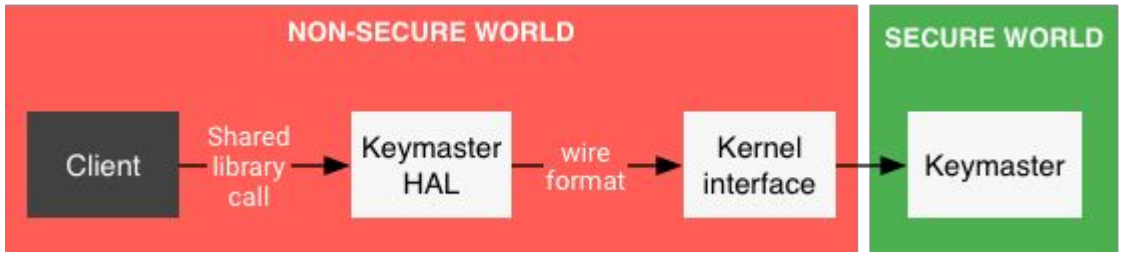
What are TEEs

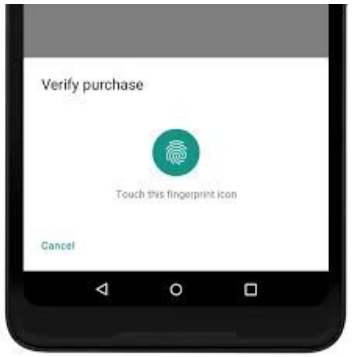

Android
TEE
TrustZone HW


Android
TEE
TrustZone HW

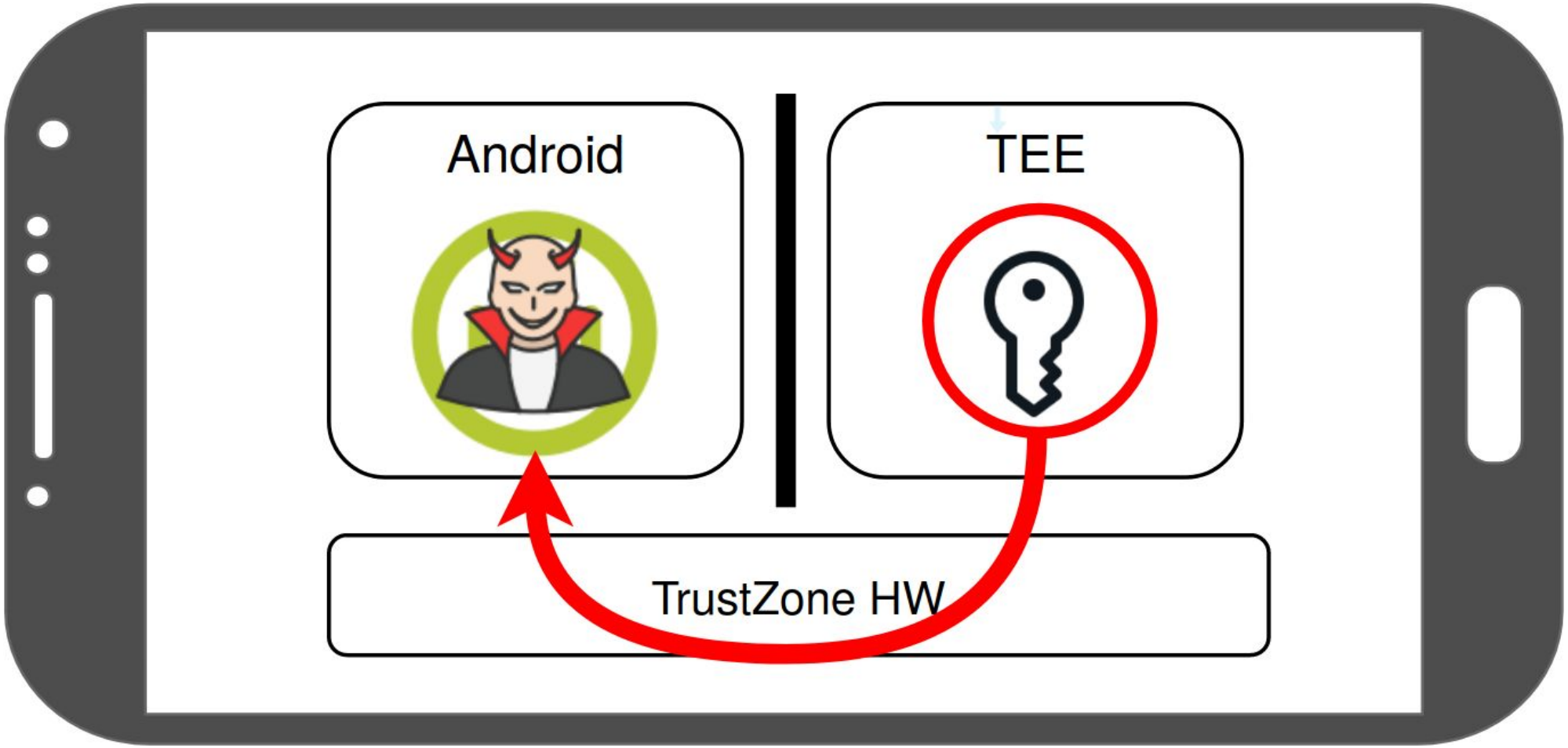
Use Cases

- 2 factor auth data
- keychain data (banking, password management…)
- private keys (gpg, signing certificates, electronic IDs, device encryption…)





What are the main problems?


Android
TEE
TrustZone HW

Android Qualcomm Vulnerability Impacts 60 Percent of Devices

Security-Oblivious Design Makes TrustZone Vulnerable to Attack

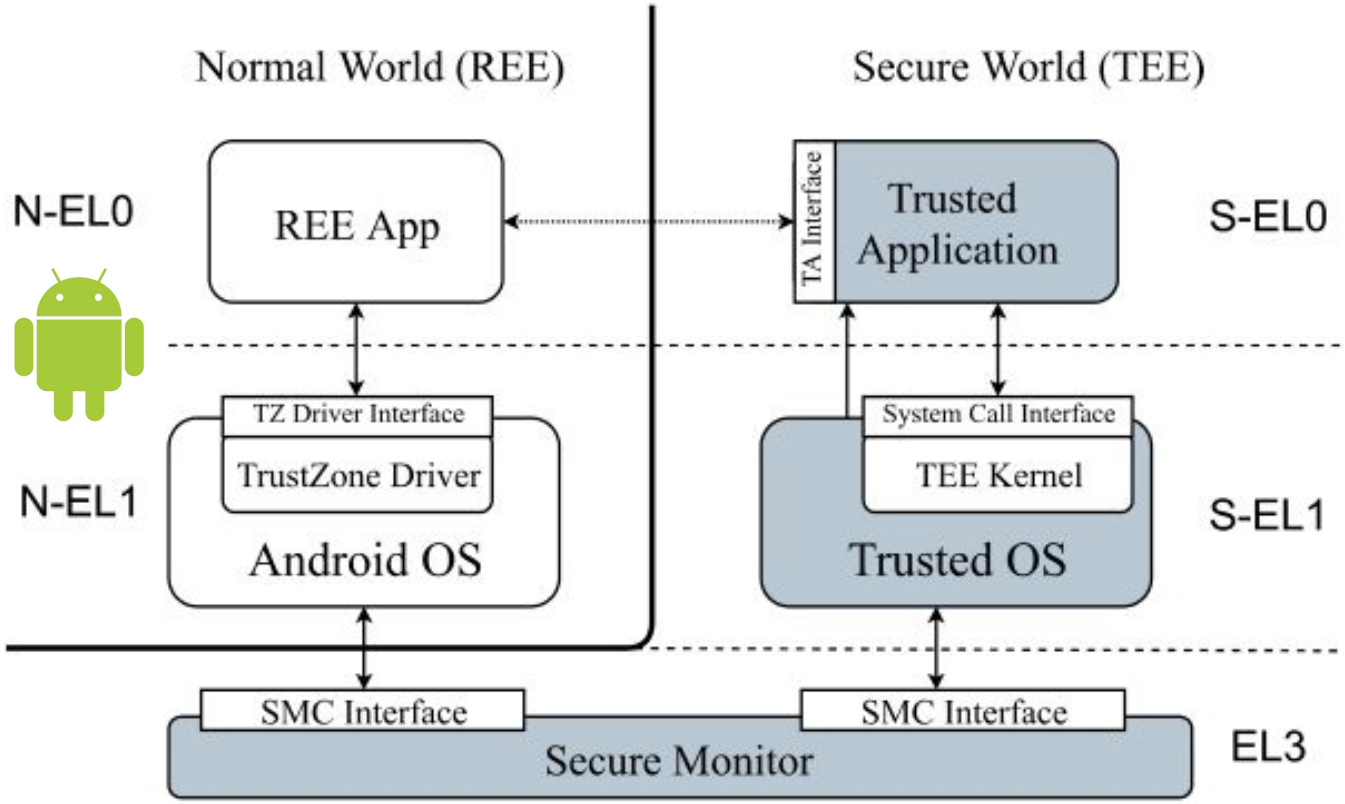
TrustZone Downgrade Attack Opens Android Devices to Old Vulnerabilities

Reflections on Trusting TrustZone

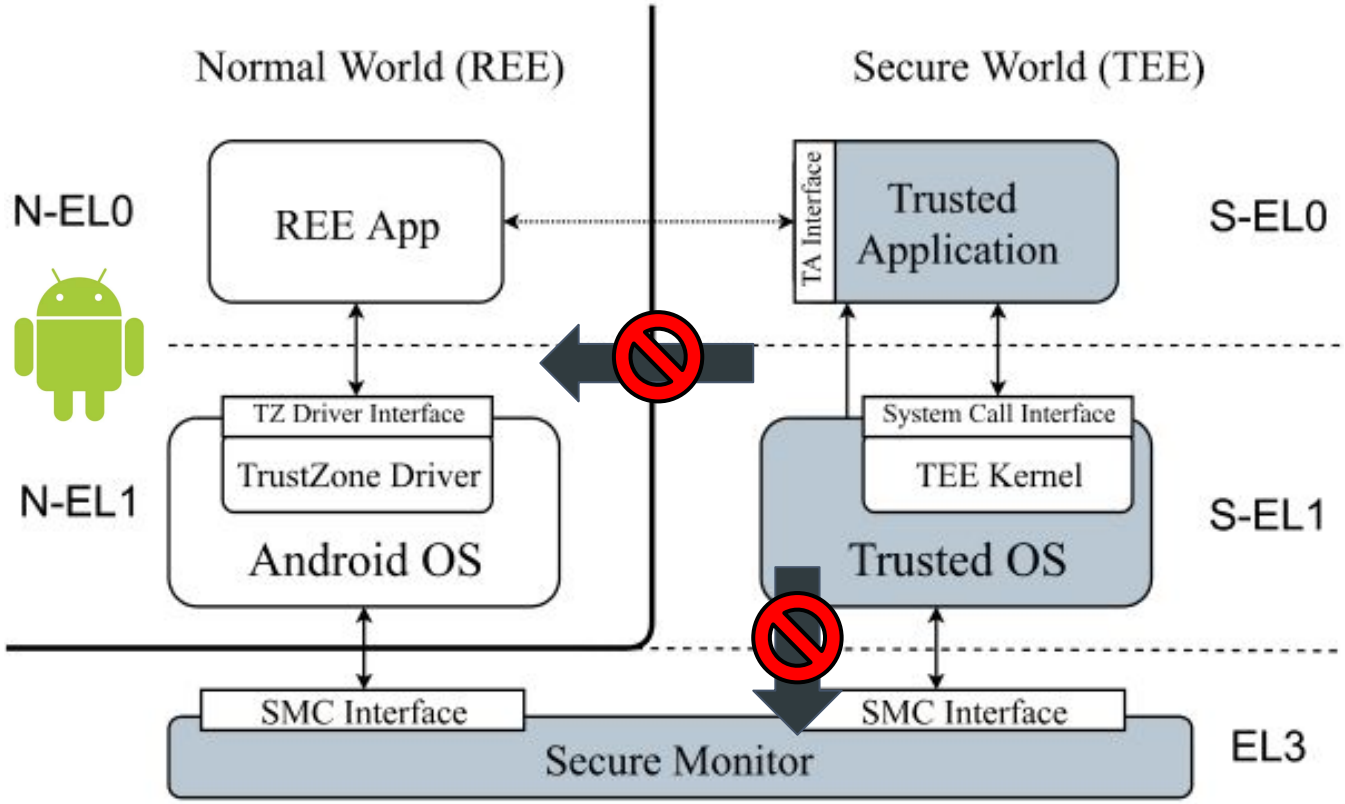
Google's full-disk encryption in Android can be hacked

BREAKING SAMSUNG'S ARM TRUSTZONE

TrustZone TEE Software Architecture



ReZone Goal


Normal World (REE)
Secure World (TEE)
N-EL0
REE App
TA Interface
Trusted Application
S-EL0
TZ Driver Interface
TrustZone Driver
Android OS
N-EL1
System Call Interface
TEE Kernel
Trusted OS
S-EL1
SMC Interface
SMC Interface
Secure Monitor
EL3

Sharing Hardware Resources is Prone to Vulnerabilities

- Micro-architectural side-channels
  - Meltdown and Spectre
  - ….
- Arm TrustZone is not immune
  - Armageddon
  - Private Key Extraction
  - Rowhammer

Software Implementation is Seldom Correct

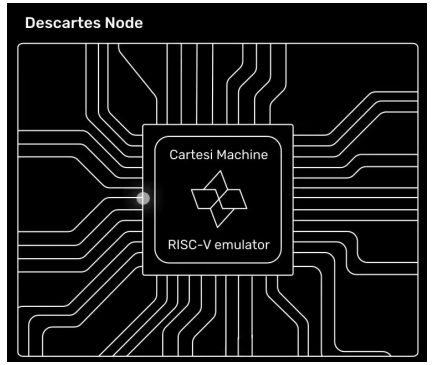
- TEEs are developed in low-level languages
  - C/C++
- Hard to write programs without bugs/vulnerabilities
- ***Many*** implementation errors

Master Thesis Proposal

Security Analysis of Cartesi

- If you'd like to explore blockchain technology
- If you'd like to learn how to identify and solve security problems
- If you'd like to learn about RISC-V
- More info
  - https://www.cartesi.io/en/docs/intro

- Cartesi uses RISC-V VMs
- Cartesi uses Linux as smart contract runtime environment



QUESTIONS?

david.cerdeira@dei.uminho.pt