

Virtualization Dungeon on ARM -  
Hands on experience talk about virtualization  
experiments



Stefan Kalkowski



# Outline

1. Motivation
2. ARM's TrustZone
3. HW-kernel library
4. Genode TrustZone
5. Demo



## Disclaimer

TrustZone is **no** virtualization solution.  
Consider ARM virtualization extensions instead!



## If marketing speaks about “Trust”

It's mostly about protection **against** the user.  
Not so much about protection **of** the user.



## Why using TrustZone in Genode?

- Started as an experiment
- Dynamic workload in “secure world”
- Sophisticated setups in “secure world”
- Running commodity OS with good performance

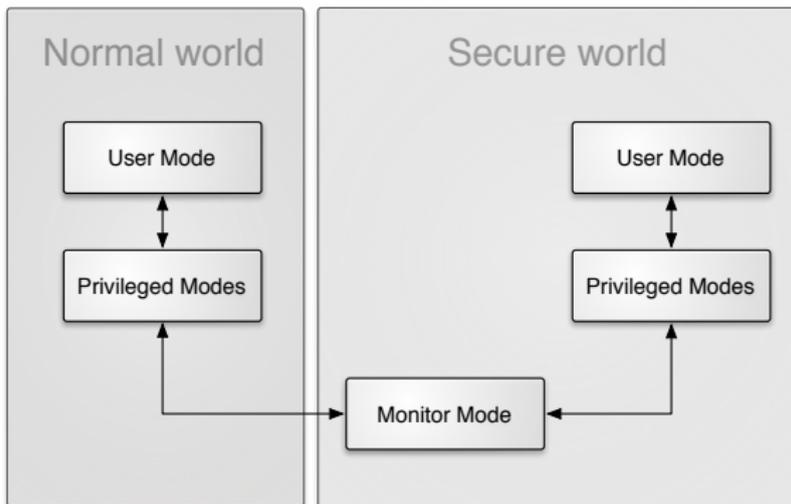


# Outline

1. Motivation
2. ARM's TrustZone
3. HW-kernel library
4. Genode TrustZone
5. Demo

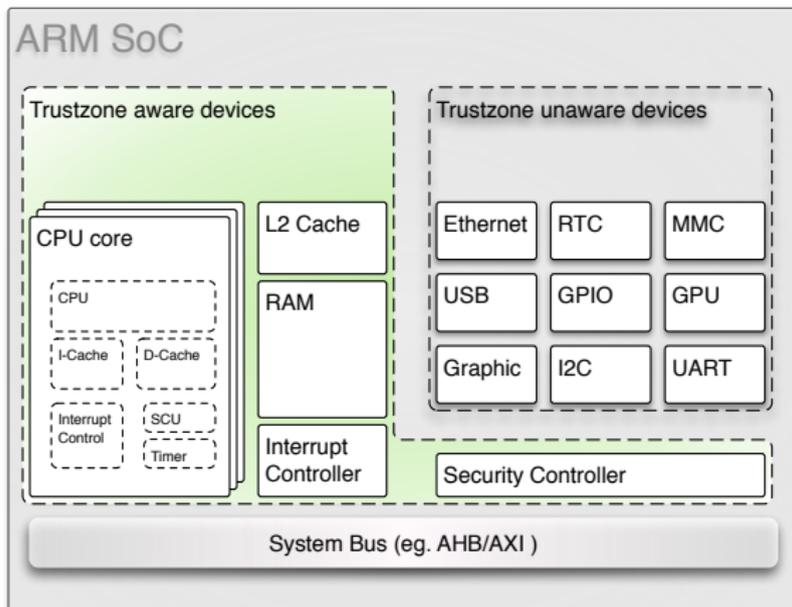


# Mostly transparent to the OS



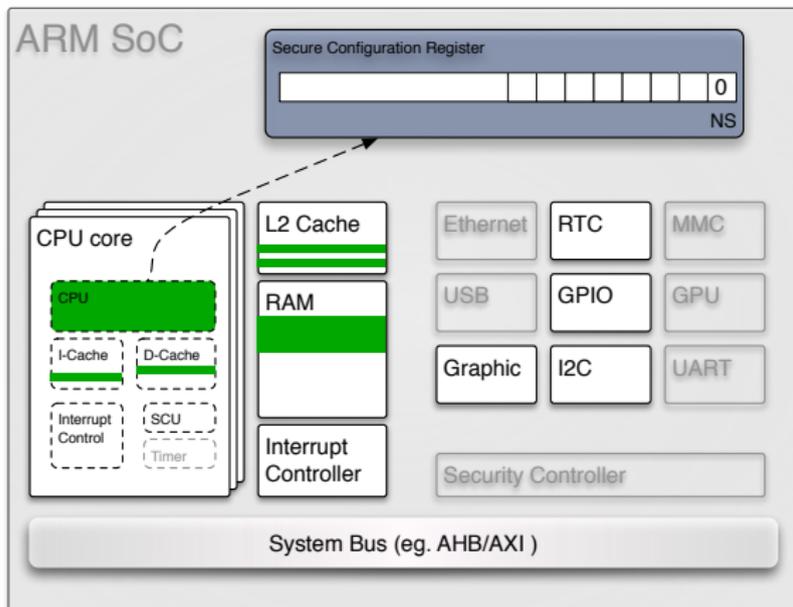


# Secure or not secure?



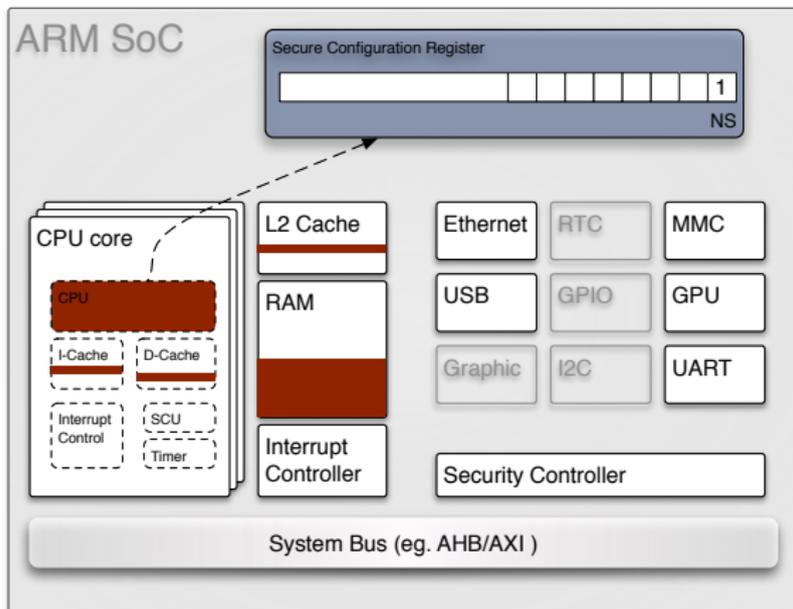


# One bit to rule them all





# One bit to rule them all



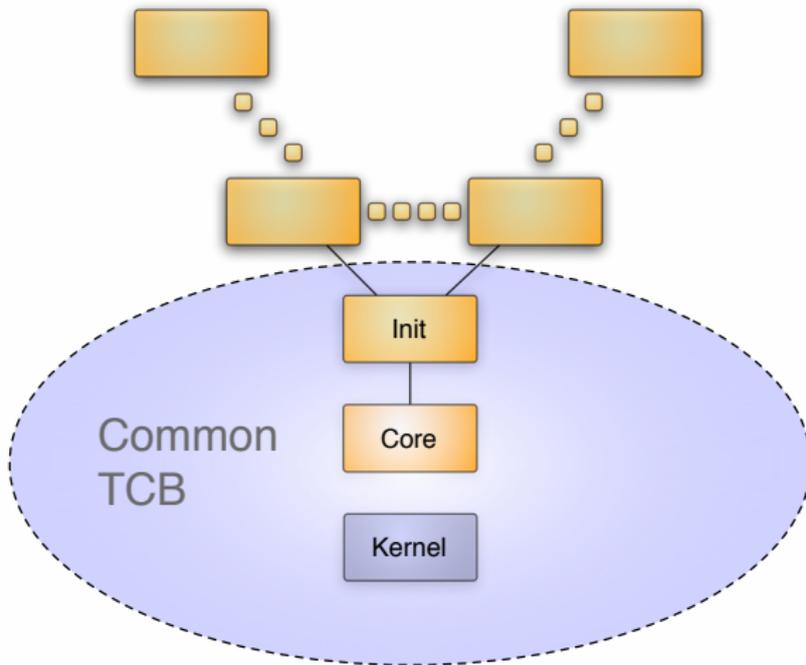


# Outline

1. Motivation
2. ARM's TrustZone
3. HW-kernel library
4. Genode TrustZone
5. Demo

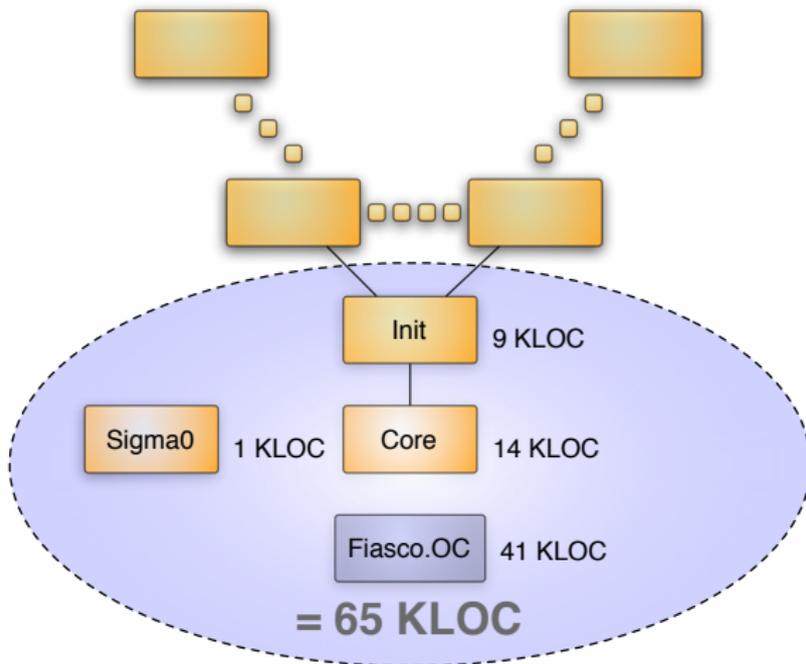


# Common Trusted Computing Base



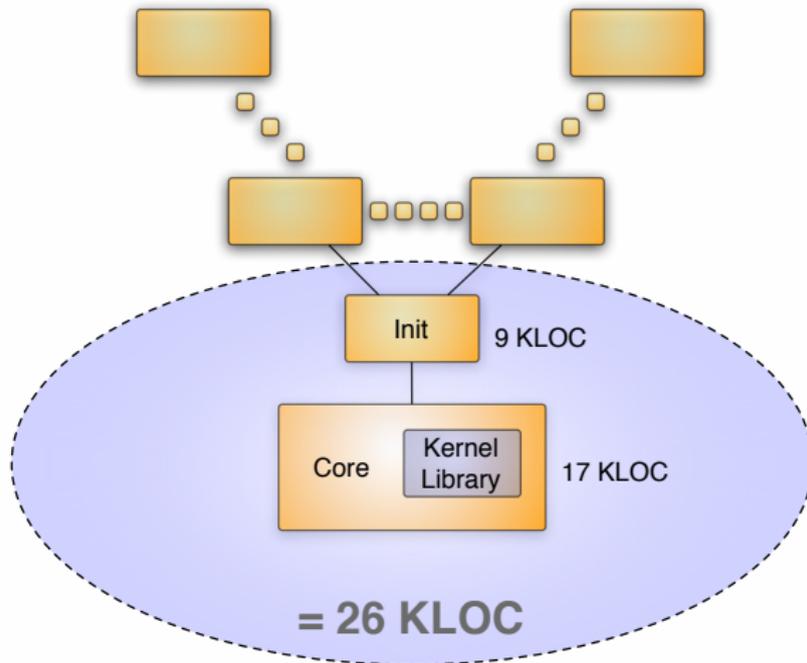


## Redundancy leads to complexity





# Genode on bare metal hardware





## HW library

- No kernel resource management problems
- TLB and cache maintainance
- Scheduling
- IRQ control
- Communication
  - ▶ IPC
  - ▶ Signals
- Various ARM CPUs and boards

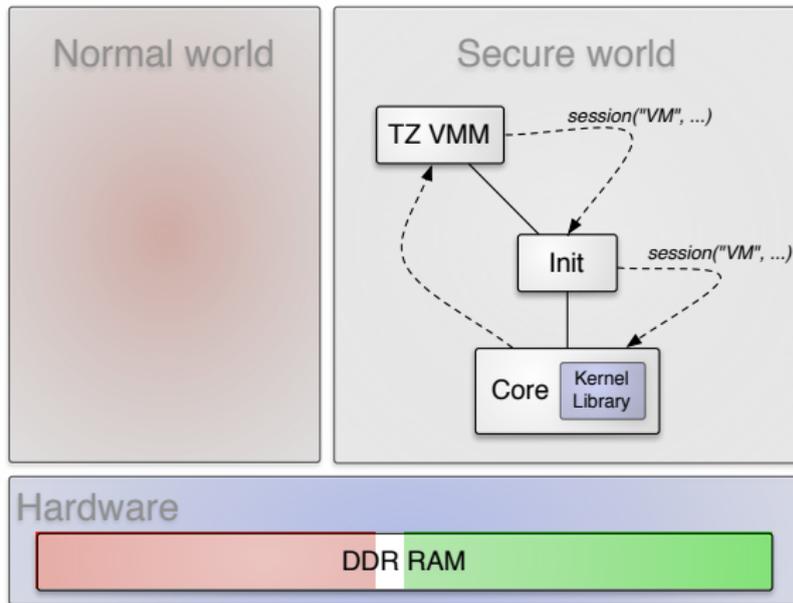


# Outline

1. Motivation
2. ARM's TrustZone
3. HW-kernel library
4. Genode TrustZone
5. Demo

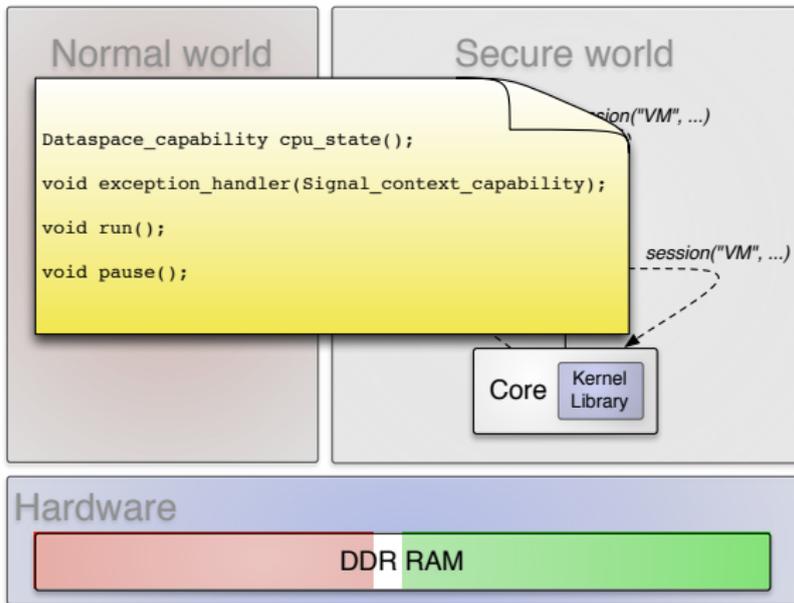


# Open VM session



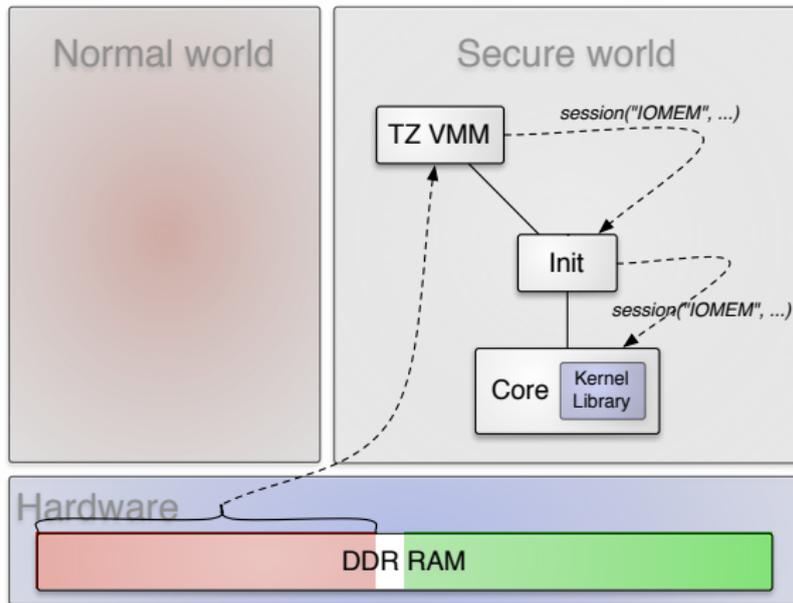


# Open VM session



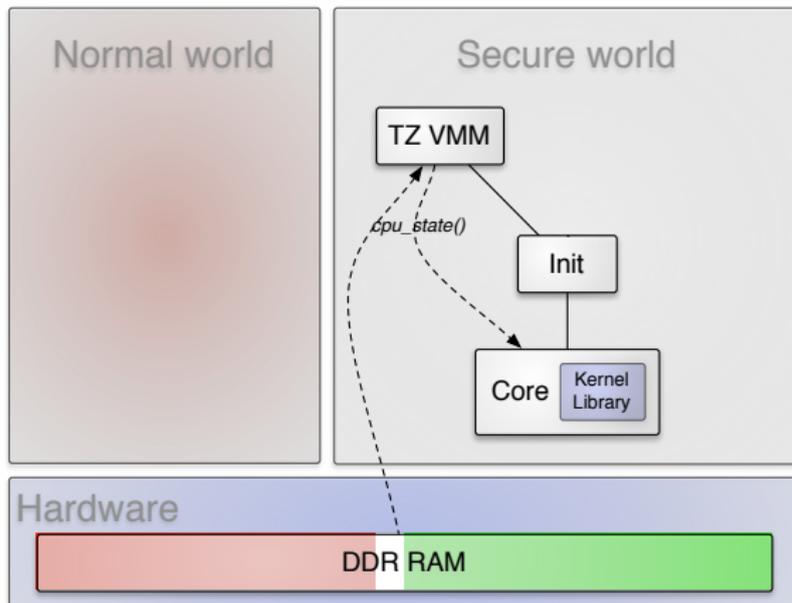


# Prepare memory



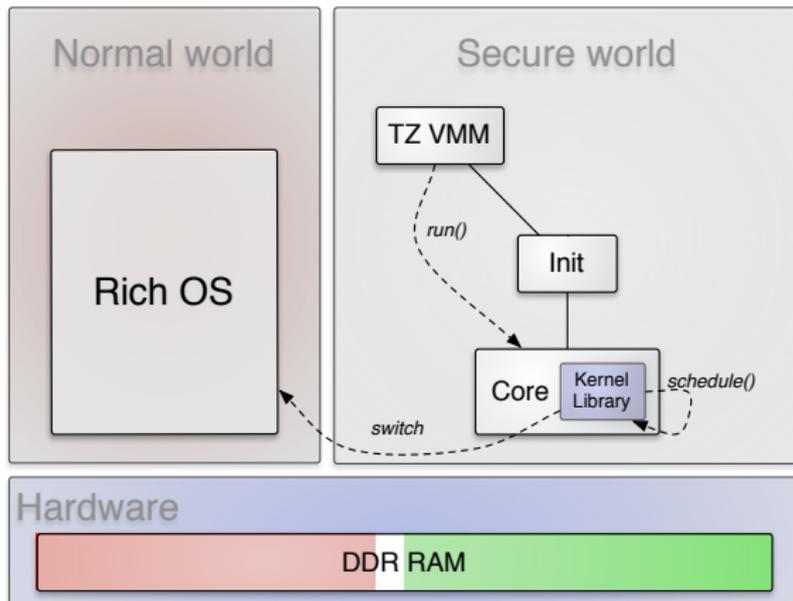


## Prepare register set





# Boot the OS



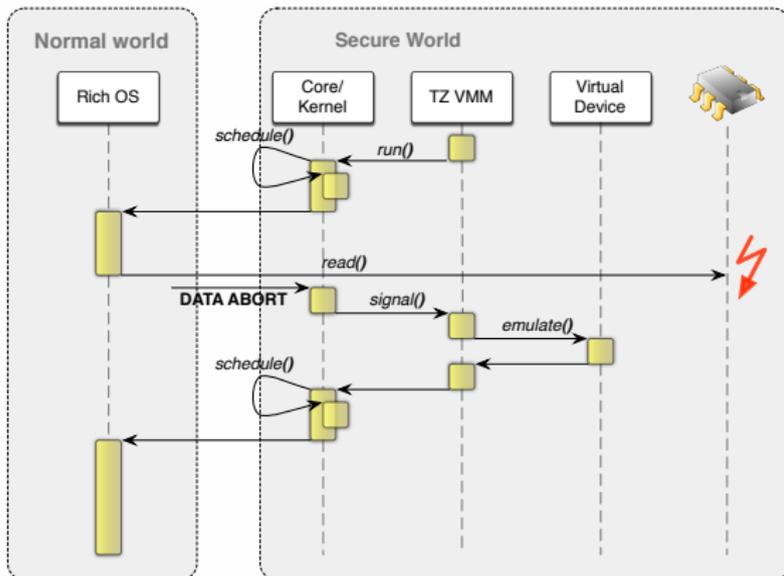


## TrustZone VMM

- Partition RAM, IRQs, and peripherals
- Act as bootloader
- Emulate devices

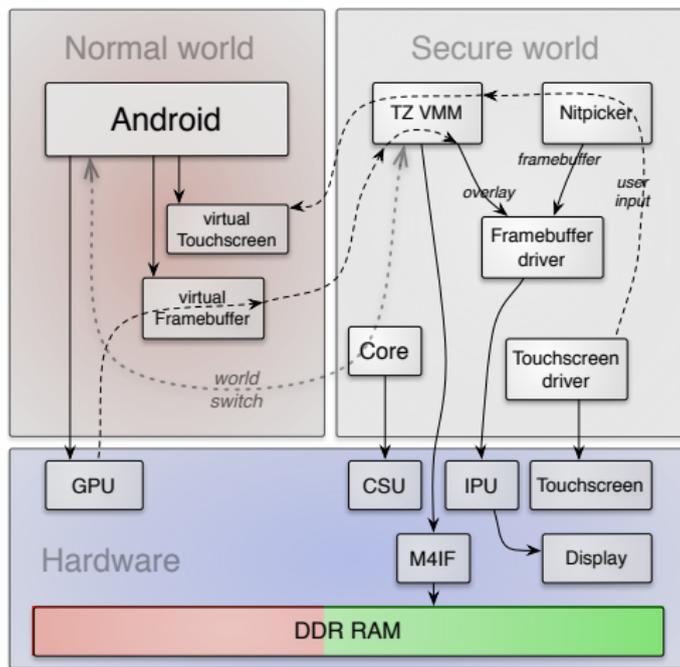


# Device virtualization





# Demo setup





## Q & A

Thank you for your attention!