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
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
1. Motivation

2. ARM’s TrustZone

3. HW-kernel library

4. Genode TrustZone

5. Demo
Mostly transparent to the OS

- Normal world
  - User Mode
  - Privileged Modes
  - Monitor Mode

- Secure world
  - User Mode
  - Privileged Modes
Secure or not secure?

ARM SoC

Trustzone aware devices
- CPU core
- Interrupt Controller
- SCU
- Timer
- L2 Cache
- RAM

Trustzone unaware devices
- Ethernet
- RTC
- MMC
- USB
- GPIO
- GPU
- Graphic
- I2C
- UART

System Bus (eg. AHB/AXI)
One bit to rule them all

ARM SoC

Secure Configuration Register

CPU core

I-Cache

D-Cache

Interrupt Control

SCU

Timer

L2 Cache

Interrupt Controller

RAM

System Bus (eg. AHB/AXI)

Ethernet

RTC

MMC

USB

GPIO

GPU

Graphic

I2C

UART

Security Controller

Virtualization Dungeon on ARM - Hands on experience talk about virtualization experiments
One bit to rule them all

ARM SoC

Secure Configuration Register

1
NS

CPU core

I-Cache D-Cache

Interrupt Control SCU Timer

L2 Cache

Ethernet RTC MMC

RAM

USB GPIO GPU

Interrupt Controller

Security Controller

System Bus (eg. AHB/AXI )

Virtualization Dungeon on ARM - Hands on experience talk about virtualization experiments
1. Motivation

2. ARM’s TrustZone

3. HW-kernel library

4. Genode TrustZone

5. Demo
Virtualization Dungeon on ARM - Hands on experience talk about virtualization experiments
Redundancy leads to complexity

\[
\text{Sigma0} \quad 1 \text{ KLOC} \quad \text{Core} \quad 14 \text{ KLOC} \quad \text{Init} \quad 9 \text{ KLOC} \quad \text{Fiasco.OC} \quad 41 \text{ KLOC} \\
\text{= 65 KLOC}
\]
Genode on bare metal hardware

= 26 KLOC

Core

Init

Kernel Library

17 KLOC

9 KLOC

= 26 KLOC
- No kernel resource management problems
- TLB and cache maintainance
- Scheduling
- IRQ control
- Communication
  - IPC
  - Signals
- Various ARM CPUs and boards
1. Motivation

2. ARM’s TrustZone

3. HW-kernel library

4. Genode TrustZone

5. Demo
Open VM session

Virtualization Dungeon on ARM - Hands on experience talk about virtualization experiments
Open VM session

Virtualization Dungeon on ARM - Hands on experience talk about virtualization experiments 18
Prepare memory

Virtualization Dungeon on ARM - Hands on experience talk about virtualization experiments
Virtualization Dungeon on ARM - Hands on experience talk about virtualization experiments
Boot the OS

Normal world

Secure world

Rich OS

Init

Switch

DDR RAM

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

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

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

Virtualization Dungeon on ARM - Hands on experience talk about virtualization experiments
Thank you for your attention!