COCONUT Secure VM Service Module

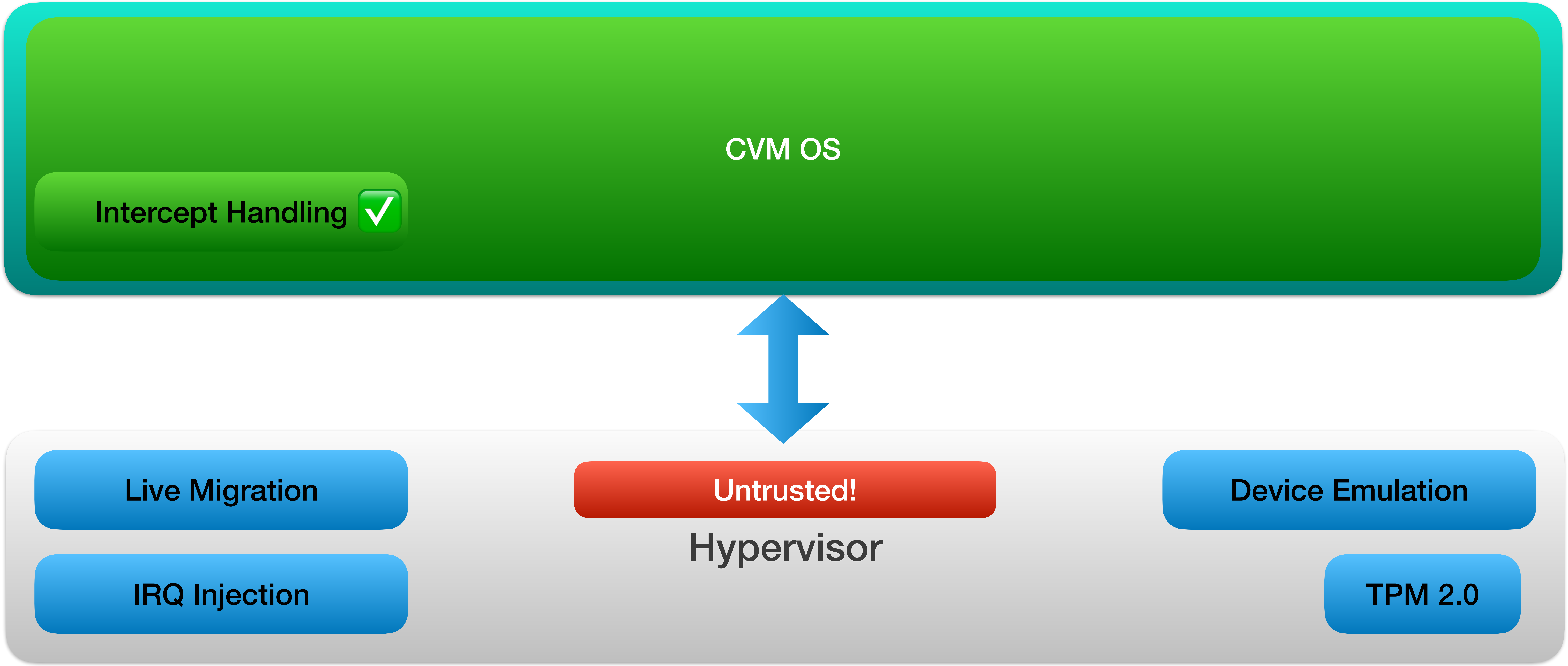
Jörg Rödel - November 30, 2023

Jörg Rödel

- Linux kernel engineer working for SUSE, former AWS and AMD
  - Working on X86 architecture and virtualization
  - IOMMUs
- Brought guest support for AMD SEV-ES to the Linux kernel in late 2020
  - That brought me into Confidential Computing
- Started a Secure VM Service Module (SVSM) project in early 2022
  - First public announcement at OC3 on March 15th, 2023
  - Called COCONUT-SVSM since publication

What is an SVSM?

CVM with Untrusted Hypervisor



CVM OS

Intercept Handling ✅

Live Migration

IRQ Injection

Untrusted!

Hypervisor

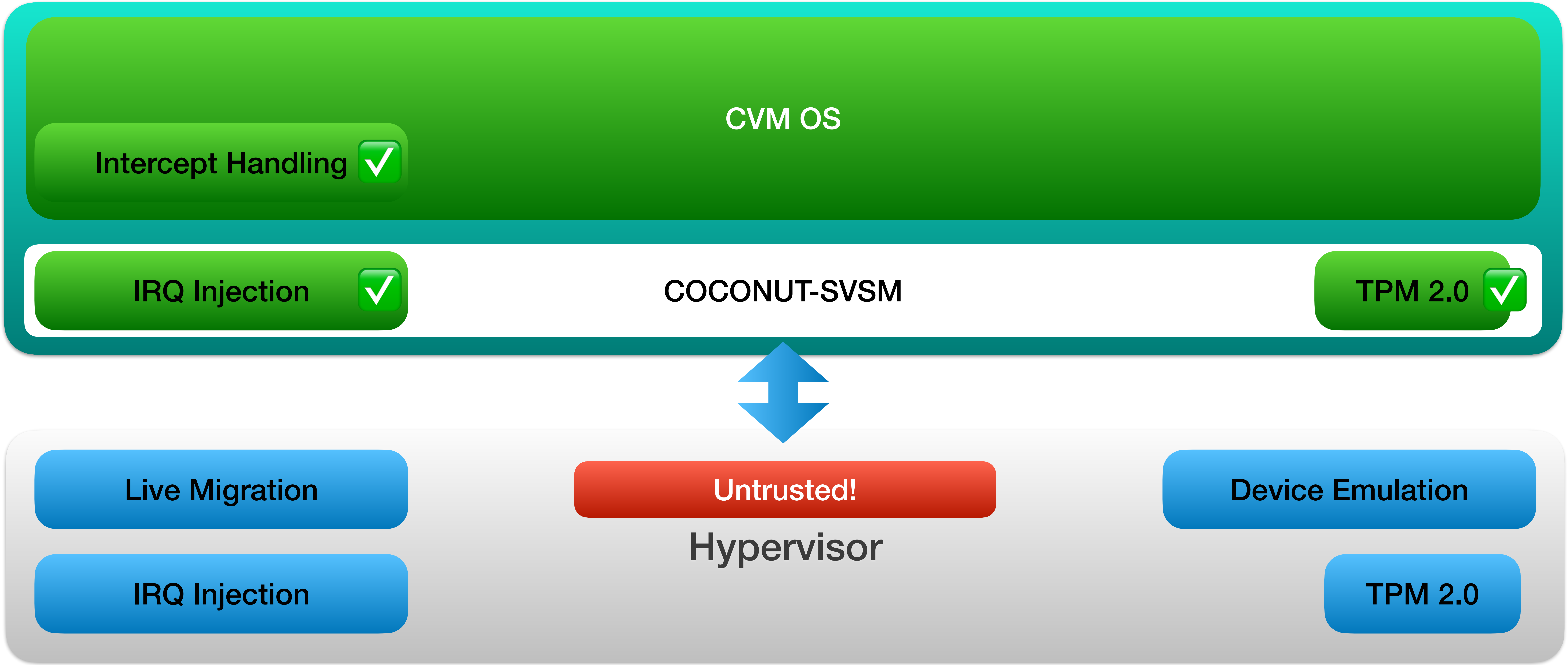
Device Emulation

TPM 2.0

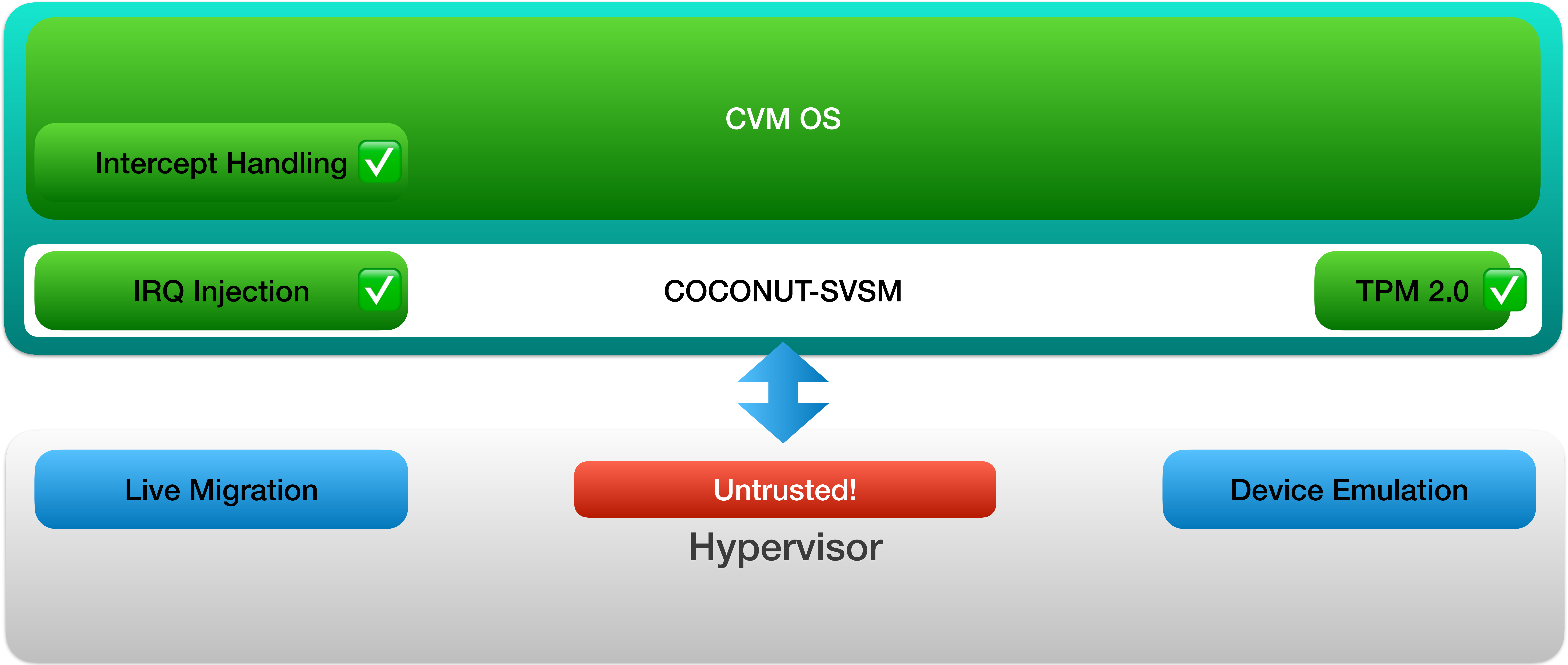
CVM with Untrusted Hypervisor

- Requires enlightened OS running in the CVM
- Huge Hypervisor (HV) interface
  - Emulated devices
  - IRQ injection
  - …
- Ongoing effort to harden guest device drivers against malicious input
- Some emulated devices carry security sensitive state (e.g. TPM)
- Alternative: Reduce the HV-Guest OS interface with an SVSM

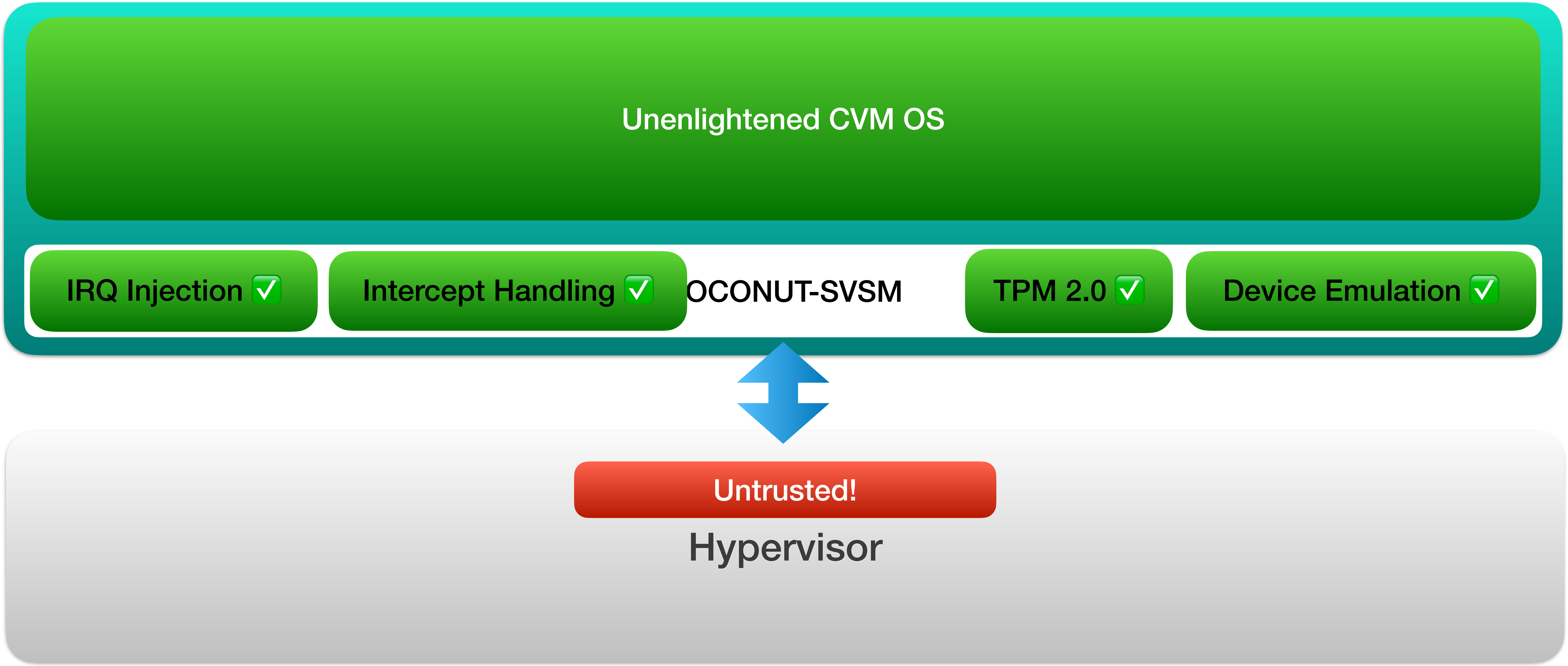
Adding COCONUT-SVSM



COCONUT-SVSM Enlightened OS Model



COCONUT-SVSM Paravisor Model



Unenlightened CVM OS

IRQ Injection ✅

Intercept Handling ✅

OCONUT-SVSM

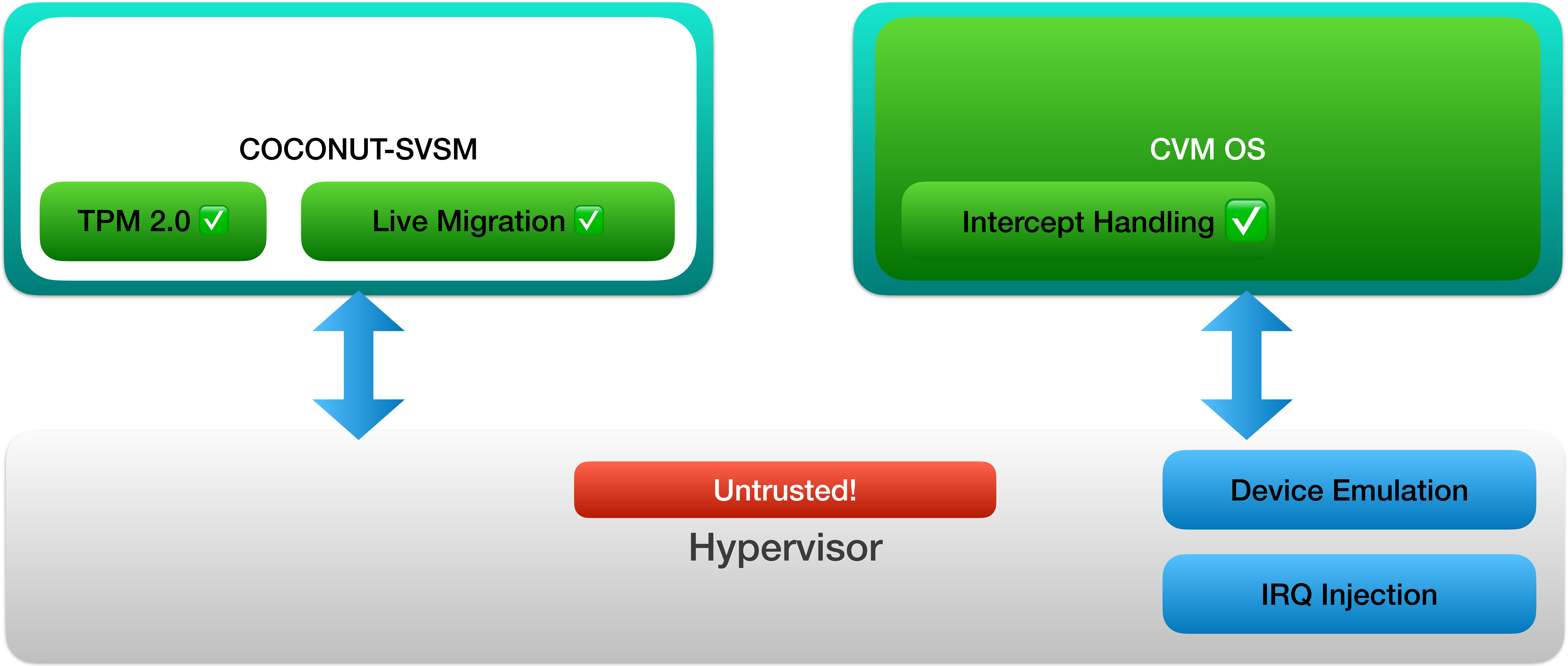
TPM 2.0 ✅

Device Emulation ✅

Untrusted!

Hypervisor

COCONUT-SVSM Service VM Model



COCONUT-SVSM

TPM 2.0 ✅

Live Migration ✅

CVM OS

Intercept Handling ✅

Untrusted!

Hypervisor

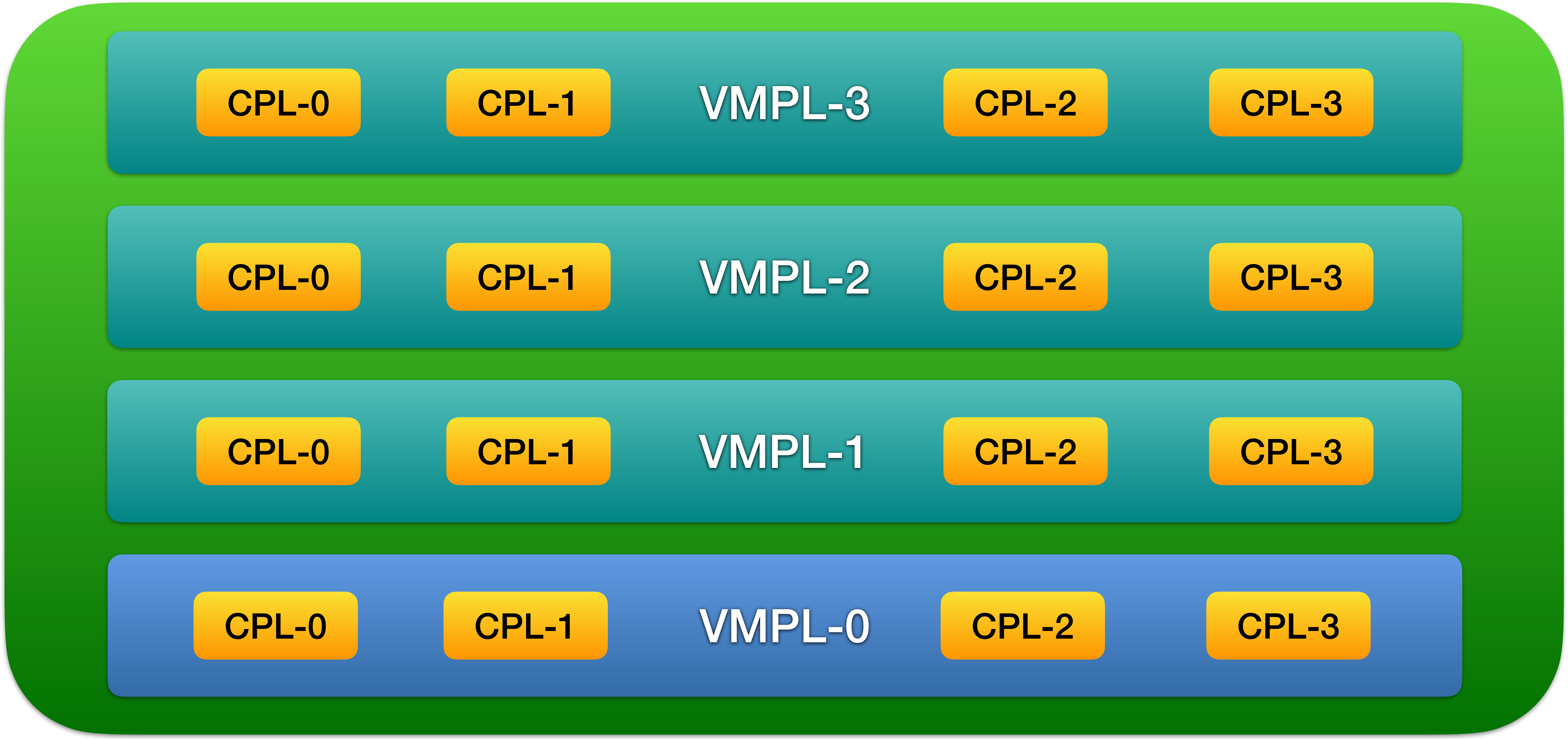
Device Emulation

IRQ Injection

Enlightened OS and Paravisor Modes

- SVSM needs memory isolation when an OS is running in the same CVM context
    - SVSM memory contains sensitive state (e.g. TPM device state)
    - OS must not have access to SVSM memory
- Memory isolation requires TEE hardware extension
    - AMD SEV-SNP: VM Privilege Levels
    - Intel-TDX: Partitioning

AMD SEV-SNP VM Privilege Levels



CPL-0 CPL-1 VMPL-3 CPL-2 CPL-3

CPL-0 CPL-1 VMPL-2 CPL-2 CPL-3

CPL-0 CPL-1 VMPL-1 CPL-2 CPL-3

CPL-0 CPL-1 VMPL-0 CPL-2 CPL-3

The COCONUT-SVSM

COCONUT-SVSM Vision

Become a generic platform for providing secure services to confidential VMs (CVMs)

- Trusted Platform Module 2.0
- Live Migration
- Variable store
- …

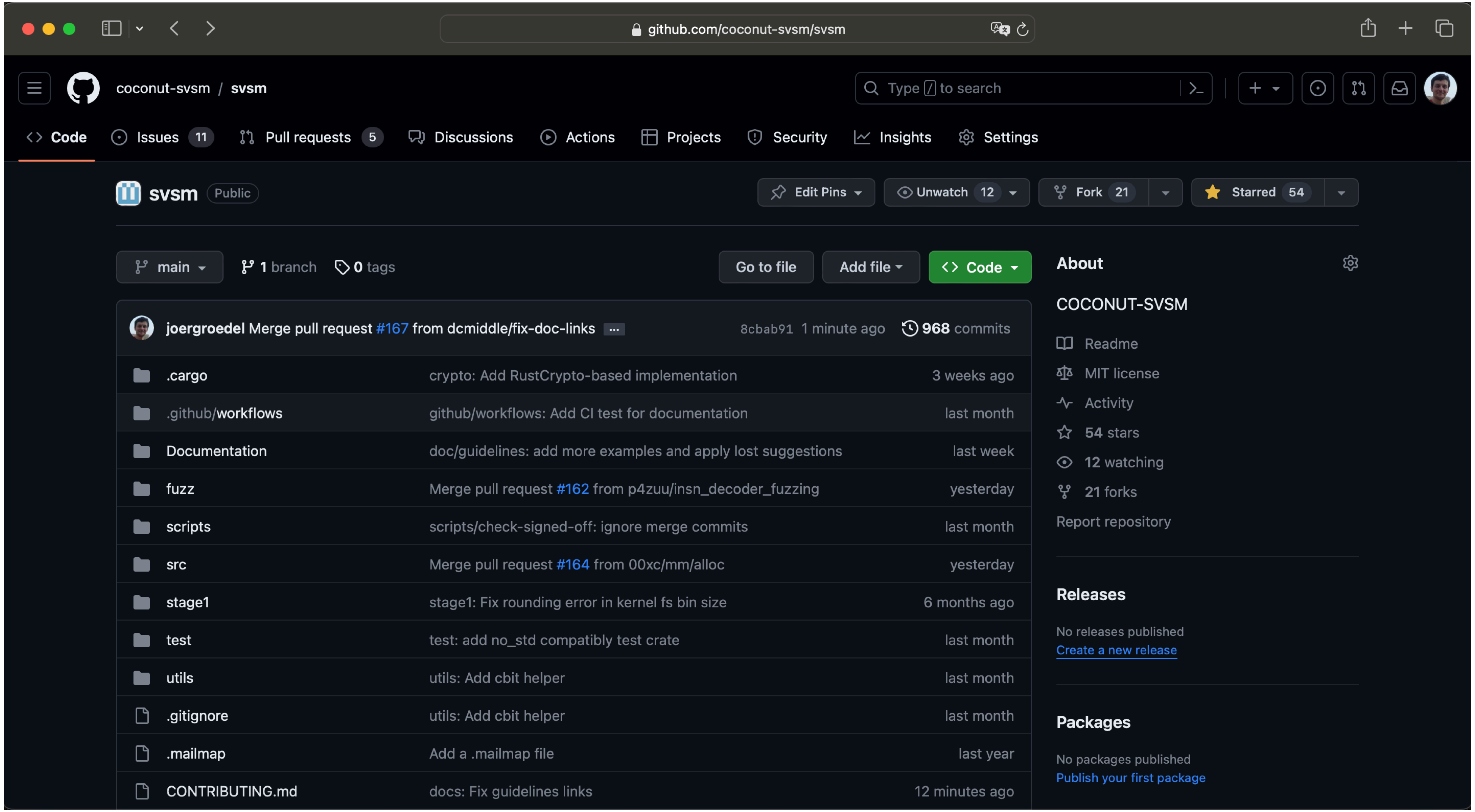
In a Nutshell

- COCONUT Secure VM Service Module - COCONUT-SVSM
- OS-level project written in Rust
- Currently ca. 15,700 LOC
- Community of 20-30 people
  - 17 code contributors to date
- Targeted at virtualization-based hardware TEEs
  - Currently runs on AMD SEV-SNP
  - Support for Intel TDX and others possible
- Strong focus on isolation

Current Features

- Boots on Linux/KVM/QEMU with Linux guest on AMD SEV-SNP hardware
- Buddy and Slab-based memory allocator
- RAM filesystem
- PerCPU page-tables
- ELF loader
- Virtual memory manager
- Basic task support
- CI: Unit-tests, Clippy, Rust-Fmt checks
- Several fuzzers

https://github.com/coconut-svsm/svsm



joergroedel Merge pull request #167 from dcmiddle/fix-doc-links … 8cbab91 1 minute ago 968 commits

.cargo	crypto: Add RustCrypto-based implementation	3 weeks ago
.github/workflows	github/workflows: Add CI test for documentation	last month
Documentation	doc/guidelines: add more examples and apply lost suggestions	last week
fuzz	Merge pull request #162 from p4zuu/insn_decoder_fuzzing	yesterday
scripts	scripts/check-signed-off: ignore merge commits	last month
src	Merge pull request #164 from 00xc/mm/alloc	yesterday
stage1	stage1: Fix rounding error in kernel fs bin size	6 months ago
test	test: add no_std compatible test crate	last month
utils	utils: Add cbit helper	last month
.gitignore	utils: Add cbit helper	last month
.mailmap	Add a .mailmap file	last year
CONTRIBUTING.md	docs: Fix guidelines links	12 minutes ago

About

COCONUT-SVSM

- Readme
- MIT license
- Activity
- 54 stars
- 12 watching
- 21 forks

Report repository

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Governance and License

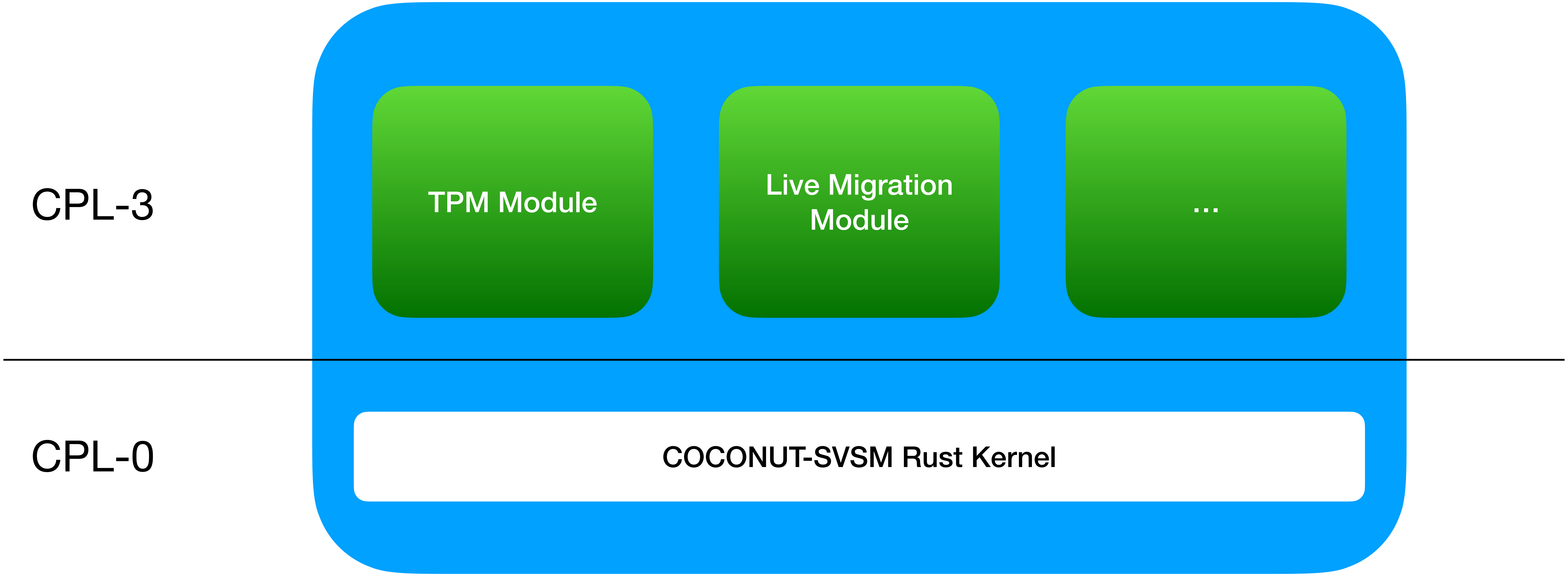
- License: MIT or Apache-2.0
- Project currently has one maintainer
    - Plan is to extend that to three
- Code changes via GitHub PRs
- Mailinglist: svsm-devel@coconut-svsm.dev
- Weekly development call
- Security bugs go to security@coconut-svsm.dev

Next Steps

Modules in User-Mode (CPL-3)

- Allows isolation of modules from the kernel and from each other
- Modules written in C, Rust, or other languages
  - Isolation from Rust kernel code base
- Modules communicate via IPC mechanism
  - Details TBD
- Users can configure COCONUT-SVSM with a custom set of modules
  - Highly adaptable to users needs

Modules at CPL-3



Next Steps for COCONUT-SVSM

- Getting CPL-3 support up and running
    - IPC mechanism
    - TPM 2.0 module as first user
- We will probably get a temporary CPL-0 TPM 2.0 implementation
    - Will make SVSM useful before CPL-3 is ready
- Persistence support
    - TPM and other services can securely store data across restarts

Next Steps for COCONUT-SVSM

- Create a module ecosystem which provide services for CVMs
  - Live migration
  - Variable store
  - Paravisor support modules
- Further improve isolation within the SVSM kernel
- Port SVSM to other TEE architectures like Intel TDX
- Port to TEEs on other hardware architectures like ARM and RISC-V

Questions?