COCONUT Secure VM Service Module Discussion
State of the Project

- Boots and runs Linux guest at VMPL-2 on AMD SEV-SNP
- SVSM Core protocol support
- Features for CPL-3 support merged:
  - ELF loader
  - RamFS implementation
  - Basic support for tasks
  - Virtual memory management data structures
- Lots of checks: RustFmt, Clippy, unit tests, Miri, fuzzing
- Currently >12000 LOC Rust code
Roadmap

• Next big milestone: Get code running at CPL-3…
  • … and run a vTPM there
  • Involves some iteration about the sys call design

• After that:
  • Get rid of the direct map
  • Persistence
  • Support booting via IGVM format
Some Open Problems
Persistence

• Design for persistence not set
  • Use a dedicated block device?
  • Need encryption and integrity protection.
  • How to get key for encryption into SVSM?
  • Access permission model?

• Deployment question
  • Store it as a separate file in the EFI partition?
Memory Management

- Getting rid of the direct map to improve isolation
- Requires changes in the allocator and page management
- Virtual address space is partitioned:
  - User
  - Per-task kernel
  - Per-CPU
  - Global shared
- Where do we need to support allocations from?
Rust Smart-Ptrs

- Currently used Rust smart ptrs just panic on allocation failure
- Not going to fly with a production SVSM
- SVSM needs smart ptrs which:
  - Can fail by returning an error
  - Use different backend allocators
- Unstable Rust smart-ptrs support all of this - but we use stable Rust
- Existing code needs to be converted to new smart ptrs
Governance

- Still ongoing discussion
- So far I am the only maintainer - goal is to get to more top-level maintainers
- Increase bus factor of the COCONUT-SVSM 😊
- Process to get there still to be discussed
Possible next steps

- Other use-cases besides vTPM:
  - Live migration
  - Variable store
  - APIC emulation and secure IRQ injection?
  - Support for more TEE architectures
  - More emulations towards paravisor support
  - Use SVSM as a platform for secure service VMs
  - Your cool idea?
SVSM BoF

- Tomorrow at **12:15PM** at **Potomac G**
- Hope to see you all here for more interesting discussions!
Open Problems Summary

• Persistence
• IGVM support
• Memory management
• Rust smart-ptrs
• Governance
• Next steps