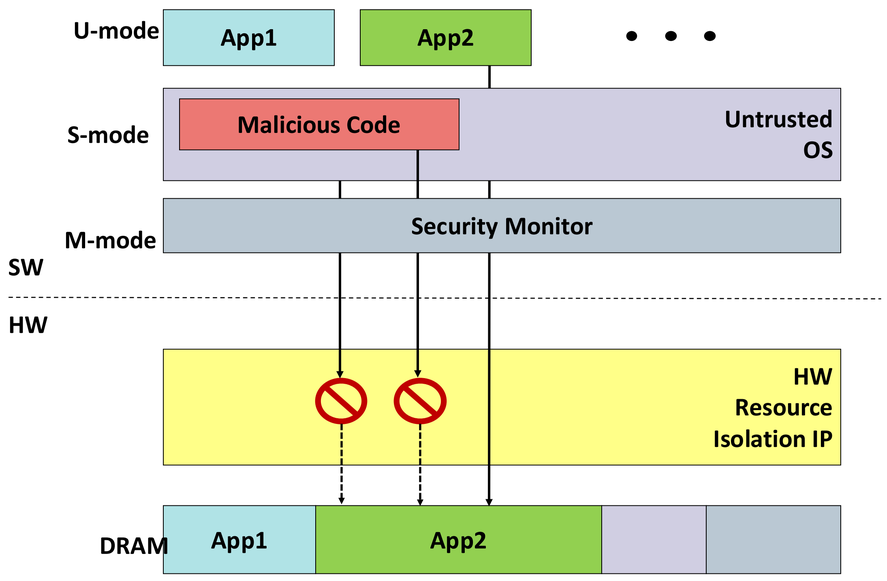
Vyond: Flexible and Rapid WorldGuard-Based Security Prototyping using Chipyard

Sungkeun Kim
Samsung Research

Hardware Isolation Primitives for Trusted Execution Environments (TEEs)

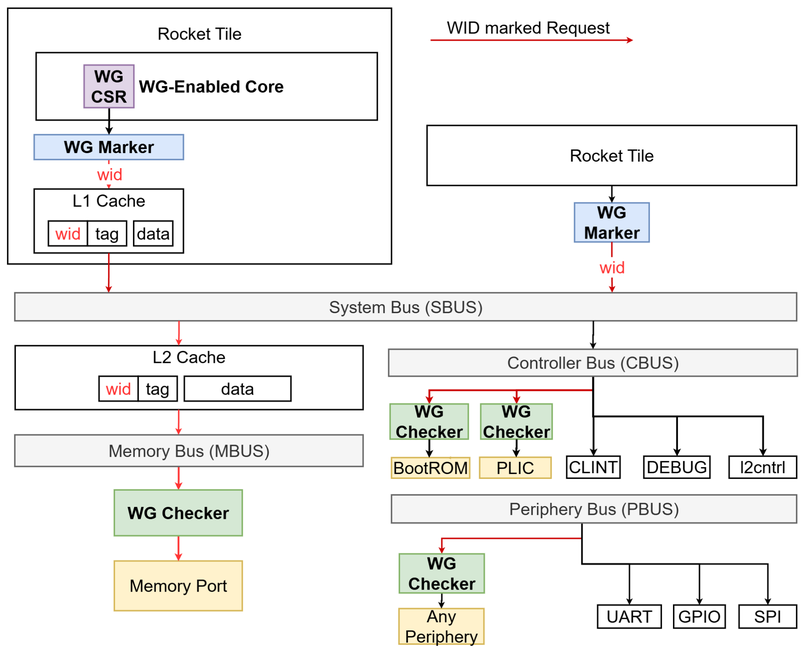
1. Prevent Unauthorized Access
Ensures that sensitive code and data are isolated from untrusted SW, including OS and hypervisor
2. Minimize Trusted Computing Base (TCB)
HW primitives enable smaller and more verifiable TCBs by enforcing boundaries at the HW level
3. Enforce Strong Access Control
HW isolation provides robust access control mechanisms that SW alone cannot guarantee



Configurable Hardware Isolation for Fast Prototyping

Security Prototyping with WorldGuard on Chipyard

1. Implemented WorldGuard Specification (v4.0)
- Implemented WorldGuard Checkers (WGC) and Markers (WGM)
- Extended Rocket Core (CSRs, TLB, and Caches), Inclusive Cache (LLC)
2. WorldGuard as Chipyard generator
- Minimum changes in Chipyard to be part of Chipyard



Key Features of Vyond

1. Generators for WorldGuard Marker and Checker
- Easy to configure and place markers and checkers

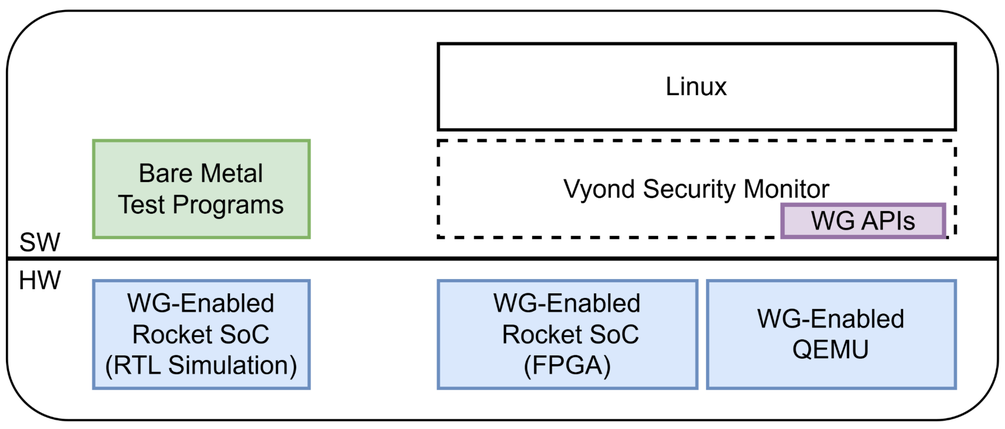
```
class WithWorldGuard(mwid: Int, widWidth: Int, nSlots: Int)
extends Config((site, here, up) => {
  case WGPLICKey => {
    Some((PLICParams(),
      WGCheckerParams(
        postfix = "wgpplic",
        mwid      = mwid,
        widWidth  = widWidth,
        nSlots    = nSlots,
        address   = 0x2040000,
        size      = 4096)
      ))
    // Other Configs such as DRAM, UART, etc..
  }
```

WorldGuard Checker Configuration for PLIC

```
trait CanHaveWGPPLICOrPlic { this: BaseSubsystem =>
  val (plicOpt, plicDomainOpt) = p(WGPLICKey) match {
    case Some((wgpParams, wgcParams)) => {
      val wgc = WGChAttachParams(wgcParams).attachTo(this)
      plic.node := wgc.node := tlbus.coupleTo("plic") {/*..*/}
      /*...*/ }
    case None => { /* Original code */ }}}
```

WorldGuard Checker Placement between PLIC and Bus

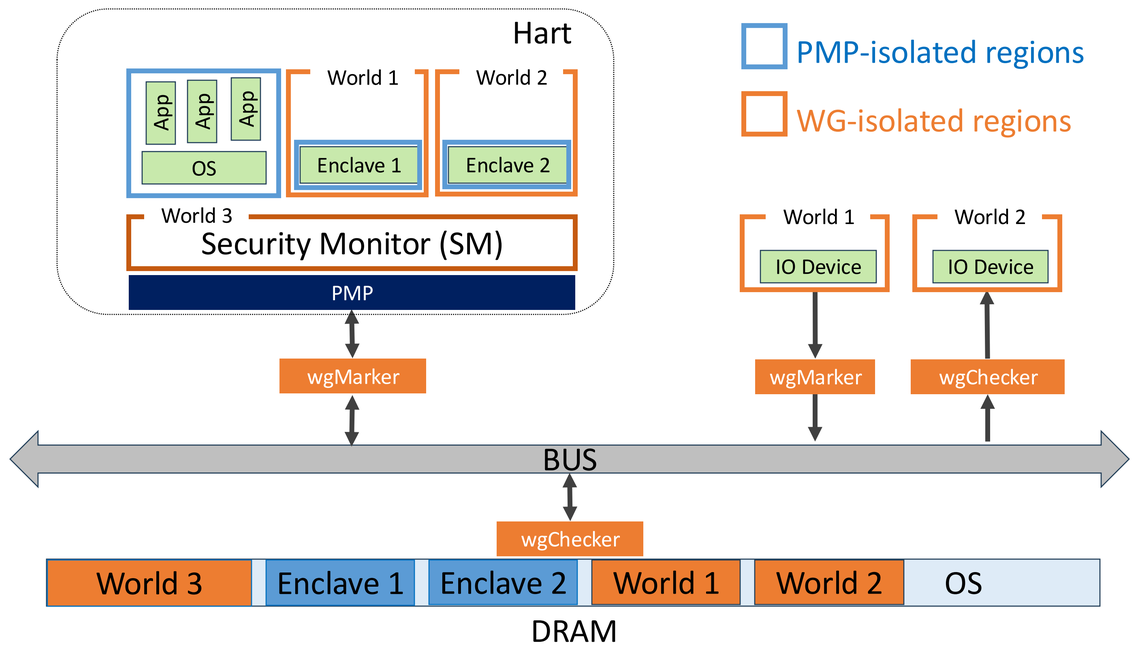
2. Support for different security design phase - Simulation, FPGA, and QEMU
- Security designer can use a proper setup depending on their design phase
3. Example configurations and test programs
- They can be references of a security monitor
- One example found a potential issue on WorldGuard specification (reported to Security TG)
4. Reference Security Monitor
- A security monitor that protects enclaves using WorldGuard (WG)



Use Cases and Future Potential

Collaboration of PMP and WorldGuard for complete isolation
- To Protect statically allocated regions (SM, I/O devices) → WorldGuard
  No extra works is required for enclave migration (e.g., PMP register update)
  Useful in Robot, Car, and IoT devices with many sensors

- To protect dynamically allocated regions (OS, Enclaves) → PMP
  As PMP is per-core solution, it is easy for SM to reallocate memory region for different enclave.



References :
1. https://lists.riscv.org/g/security/attachment/711/0/worldguard_rvia_spec-v0.4.pdf
2. https://github.com/ucb-bar/chipyard
3. https://patchwork.ozlabs.org/project/qemu-devel/cover/20240612081416.29704-1-jim.shu@sifive.com

Contact :
https://www.github.com/Samsung/vyond
sk84.kim@samsung.com