RISC-V Summit 2018

SiFive's Trusted Execution Reference Platform

Palmer Dabbelt, Nate Graff

RISC-V Summit: December 5th, 2018

"Can I get a RISC-V U2F token?"

"RISC-V doesn't have ARM TrustZone, we can't use it."

"How do I isolate private data?"

RISC-V needs a comprehensive playbook for implementing secure embedded computing solutions.

"How do we protect against side-channel attacks?"

"Can RISC-V do secure boot?"

SiFive

What is a Trusted Platform?

- **Secure Boot**
  - Control the software executing on a machine
- **Private Storage**
  - A place to store cryptographic keys
- **Tamper-Evident Storage**
  - A place to store the time the system was shut down
- **Remote Attestation**
  - Can I trust the target to do compute for me?
- **Side-Channel Attacks**

Three questions to answer:

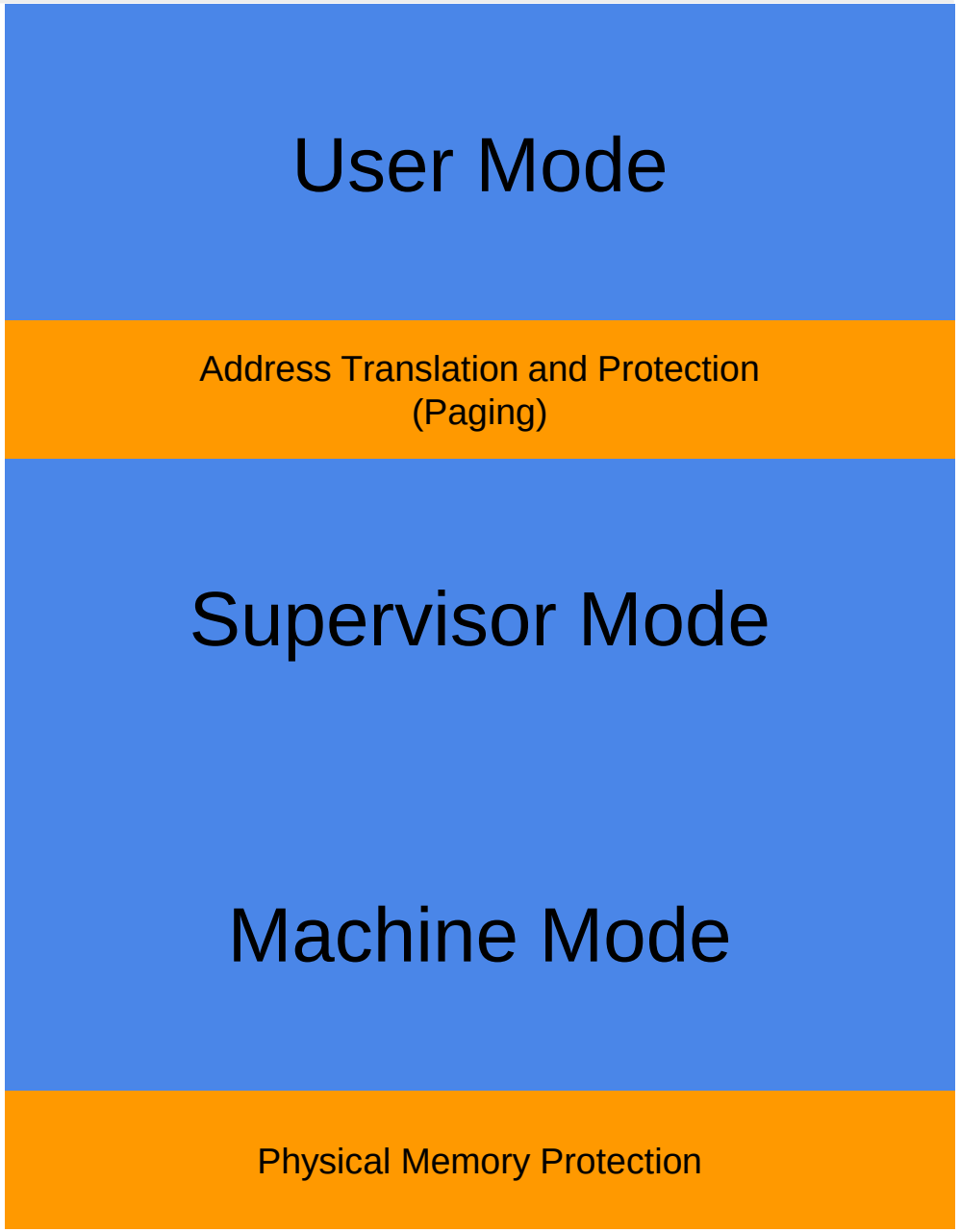
Can **RISC-V** systems provide a **comprehensive** solution to **secure** embedded computing?

What are the **components** of a secure embedded RISC-V system?

How do we know when we have **all the components** we need?

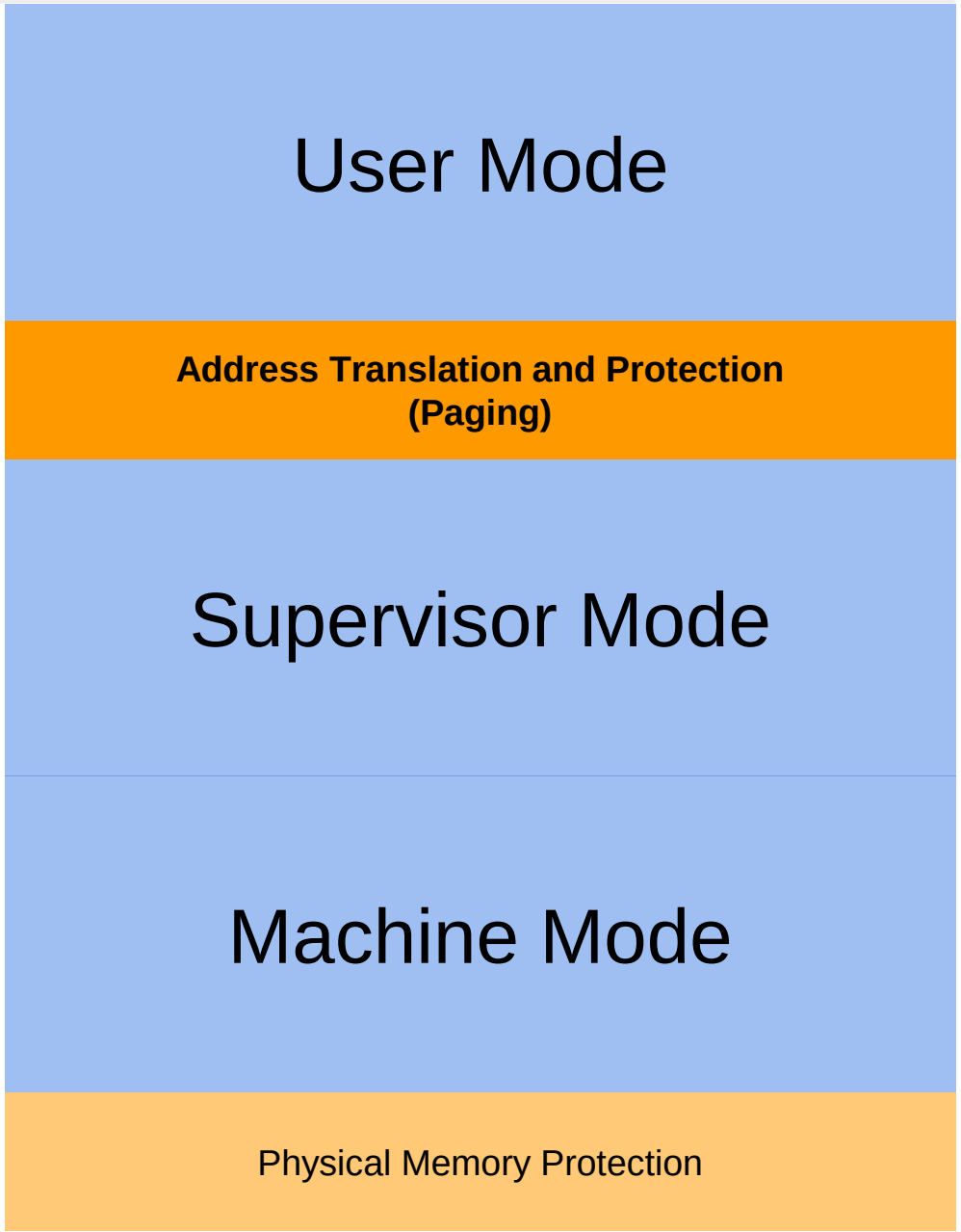
What does RISC-V Have Now?

- **3 modes in RISC-V ISA**
  - User, Supervisor, and Machine
- **Two protection boundaries**
  - Supervisor protected from user
  - PMPs protect all accesses
- **Address translation and protection**
  - Standard page-based scheme
- **Physical memory protection**
  - Base+bounds scheme
  - No translation
  - Protect all accesses



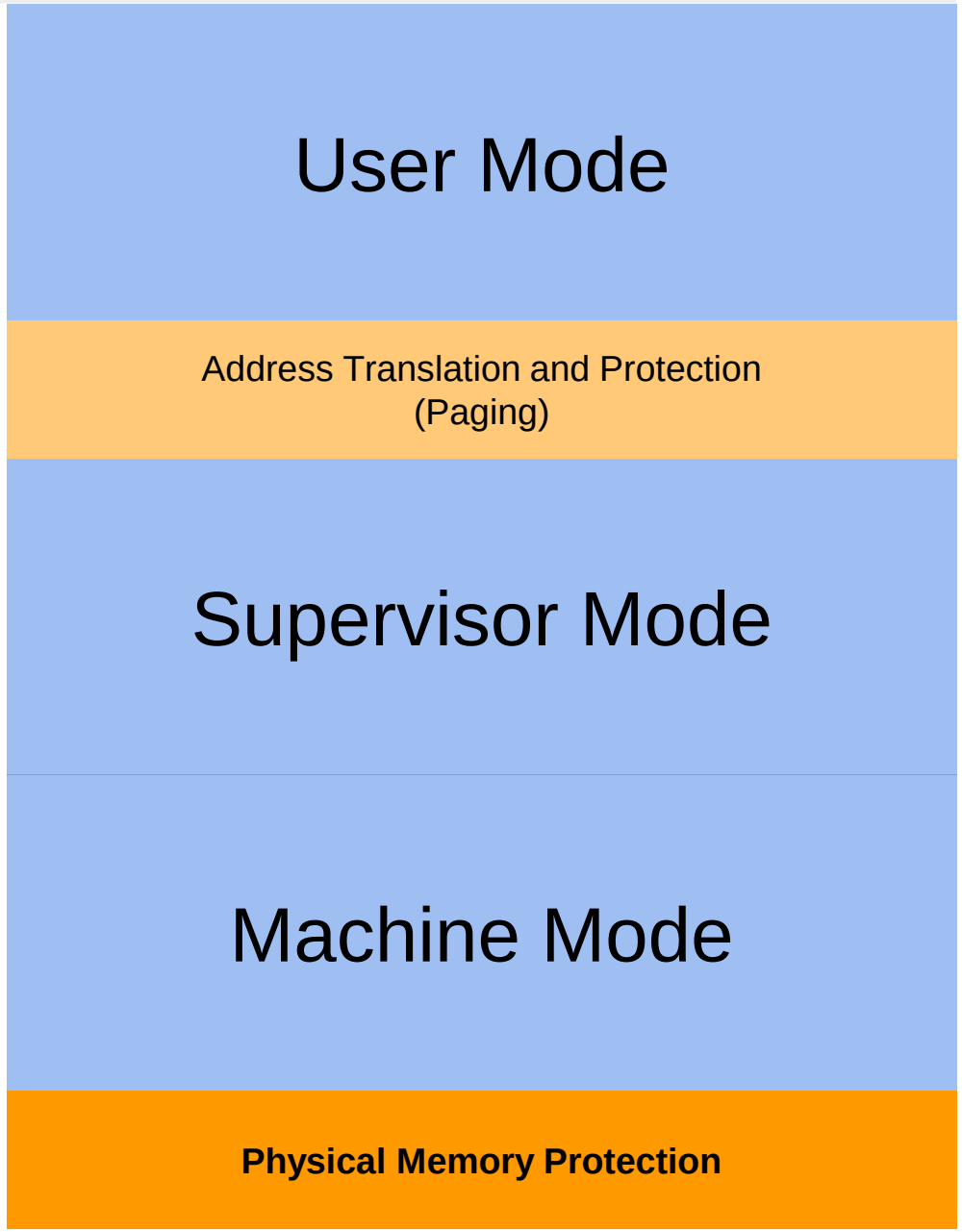
Paging on RISC-V Systems

- **SATP CSR**
  - Per-hart page table base pointer
- **Between user and supervisor**
  - Single register
- **Standard-looking scheme**
  - Normal forward paging
  - 4KiB pages for 64-bit systems
  - Various larger pages, global pages, accessed/dirty bit, etc
- **Support for extension**
  - Standard paging is defined in the ISA
  - Bits remain for extensibility



Physical Memory Protection (PMP)

- **PMP CSRs**
  - Per-hart page table base pointer
- **Protection for all accesses**
  - User, supervisor and machine
  - Protection only, no translation
- **Region-based scheme**
  - CSR value defines region size and shape
  - Up to 16 regions
- **Software configurable**
  - Writable by machine-mode software
  - Can be locked until system reset
- **Protection for machine-mode only implementations!**



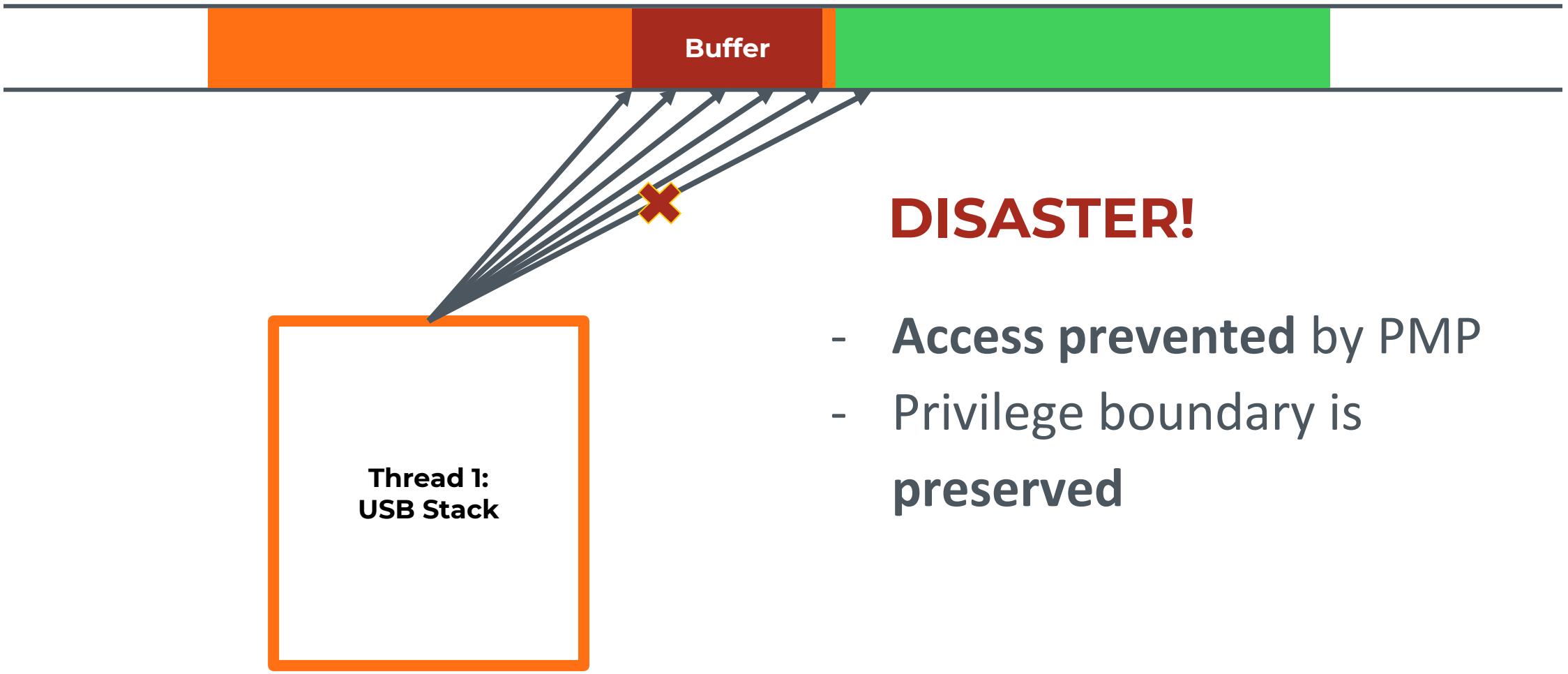
Physical Memory Protection (PMP)

Access to memory regions granted by
PMP configuration

Thread 1:
USB Stack

Thread 2:
Crypto Runner

Physical Memory Protection (PMP)



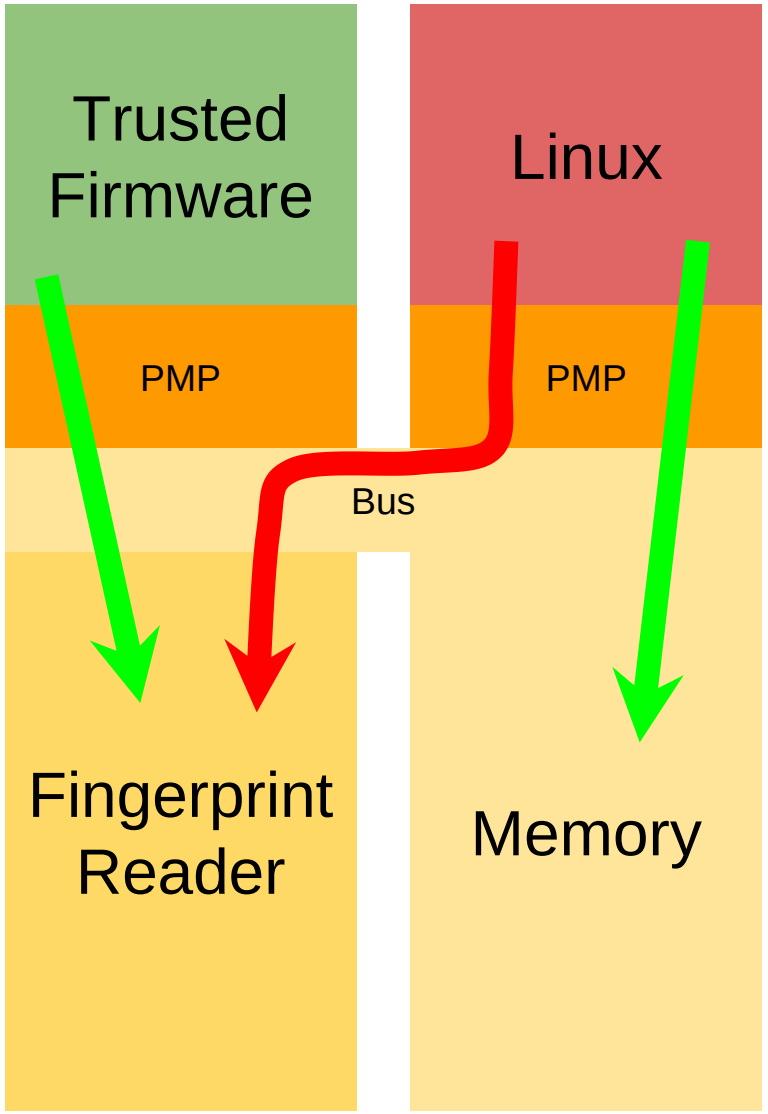
DISASTER!

- **Access prevented** by PMP
- Privilege boundary is **preserved**

Example PMP Uses

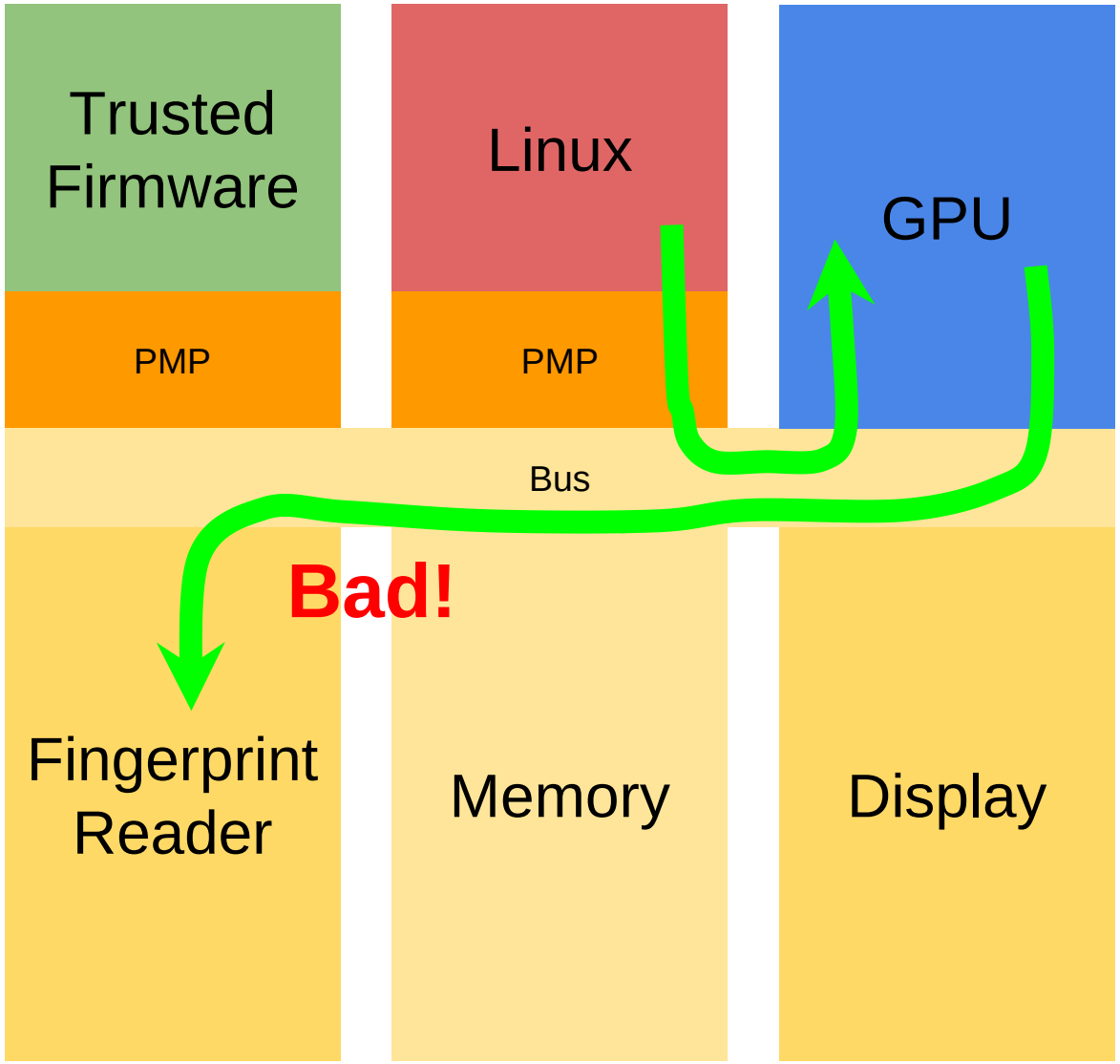
- **Time multiplex multiple programs without paging**
  - Programs can run in user mode without supervisor mode
  - PMPs can protect programs from each other
- **Protect devices from untrusted supervisor-mode programs**
  - PMPs protect all physical accesses per mode
- **Protect and share memory in multi-CPU programs**
  - PMPs are per-hart configurations
  - Up to 16 regions
- **Disable a device until a reboot**
  - PMPs can be locked, disabling a device from even machine mode
- **Protection for machine-mode only implementations!**

Protection from Bus-Mastering Devices



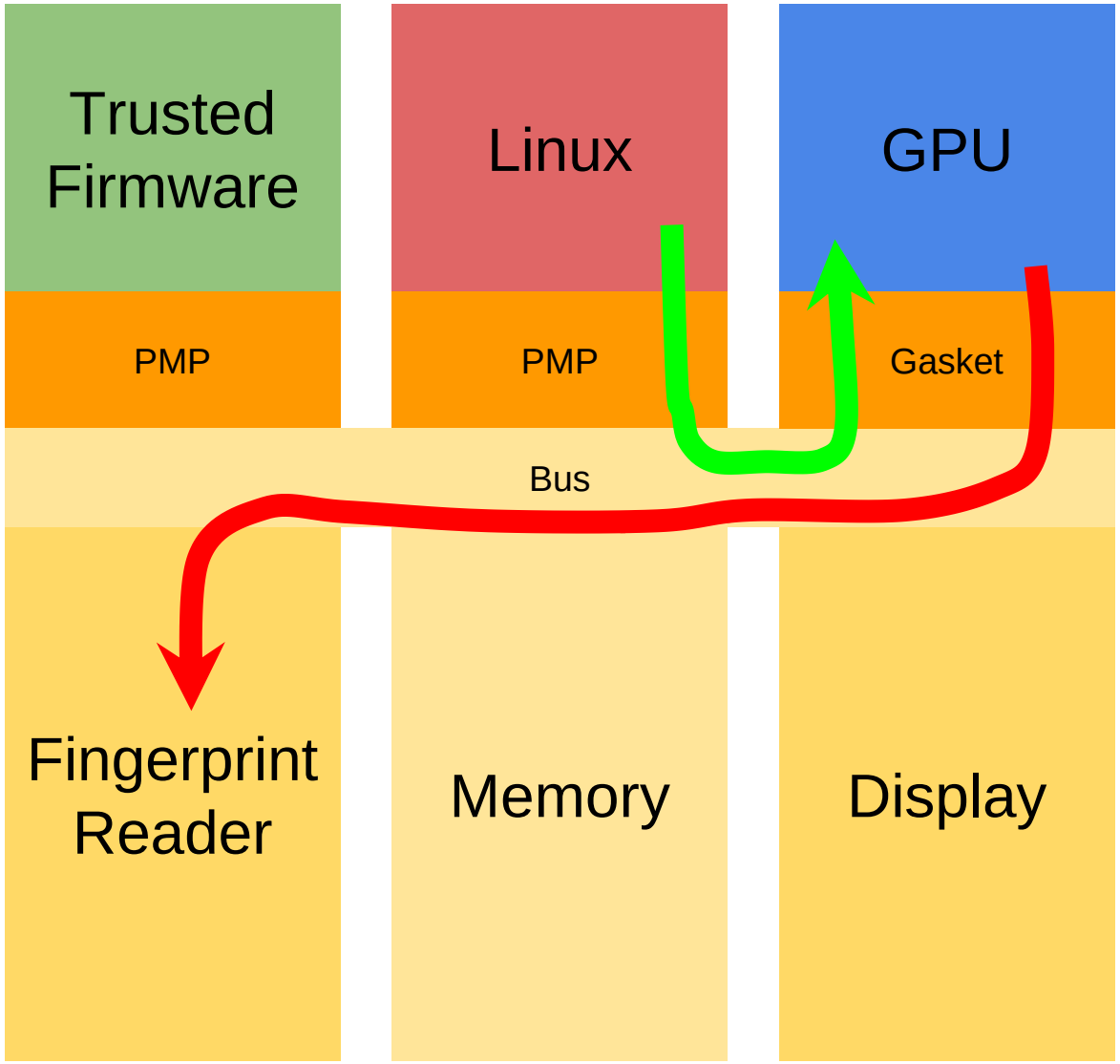
- **PMPs apply to all accesses from a CPU**
- **Devices can be protected by address**
  - Protections are per privilege mode
- **Doesn't require trusting the bus**
  - Accesses are mandated by the CPU
- **Similar scheme for protecting buffers**
  - PMPs just protect ranges

Gaskets: PMPs for Devices



- **PMPs only apply to CPUs**
  - Bus mastering devices can access memory too

Gaskets: PMPs for Devices



- **PMPs only apply to CPUs**
  - Bus mastering devices can access memory too
- **Gaskets for other masters**
  - Memory-mapped PMPs
  - Same protecting scheme
- **Not a RISC-V specification**
  - A SiFive specification
  - Available in FU540-C000 (on the HiFive Unleashed)

Writing Trusted Software

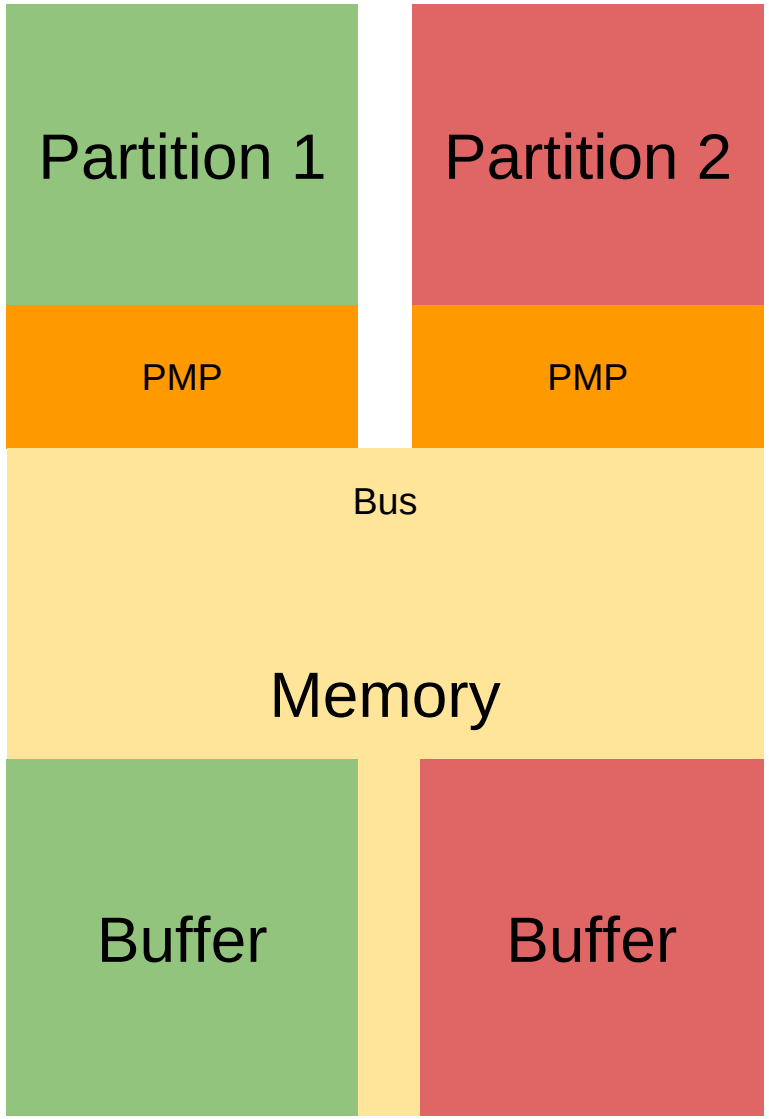
- **Hardware mechanisms allow us to limit trust placed on software**
- **Software must have a hardware root of trust**
- **Physically Unclonable Function (PUF)**
  - Enables a per-device secret cryptographic key
  - Physical devices cannot be cloned
  - “Sanctum: Minimal Hardware Extensions for Strong Software Isolation”
  - Must be implemented in hardware
- **Protection against physical attacks**
  - Reset timing attacks, clock attacks, power attacks, etc
  - DRAM encryption

Trusted Reference Platform

- **Runtimes are written to a platform more than to an ISA**
- **We need a specification to allow for portable software**
- **Some ISA-related concerns**
  - Privilege modes
  - Existence of PMPs
  - Resistance to speculative side
- **Many platform-related concerns**
  - Gaskets and bus blockers
  - Reset sequence for secure boot
  - Presence and detection mechanism for a PUF
- **ISA specifications aren’t sufficient, we need a platform spec!**

SiFive Trusted Firmware

- **Static partitioning of SOC**
  - Multiple security zones
  - Time multiplexing of payloads
- **Evaluation of trusted platform spec**
- **Designed to be simple and portable**
  - Suitable as an example
  - Useful for simple systems
  - Proof of concept for the platform
- **Berkeley Keystone Talk**
  - Active research in security monitors
  - 3:30pm Today in Room 209/210
- **HexFive Security Monitor**
  - Demos on the show floor



Demo!

- **SiFive's Freedom U54 CoreIP**
  - Same IP on the FU540-C000 ASIC
- **Rambus CryptoManager IP**
  - Hardware root-of-trust (PUF)
- **Secure Boot of Linux-Based System**