Research Projects@COMPASS

Fengwei Zhang

RISC-V Security

1. Pointer Integrity
   - Protecting return address

2. Memory Boundary Protection
   - Out of boundary

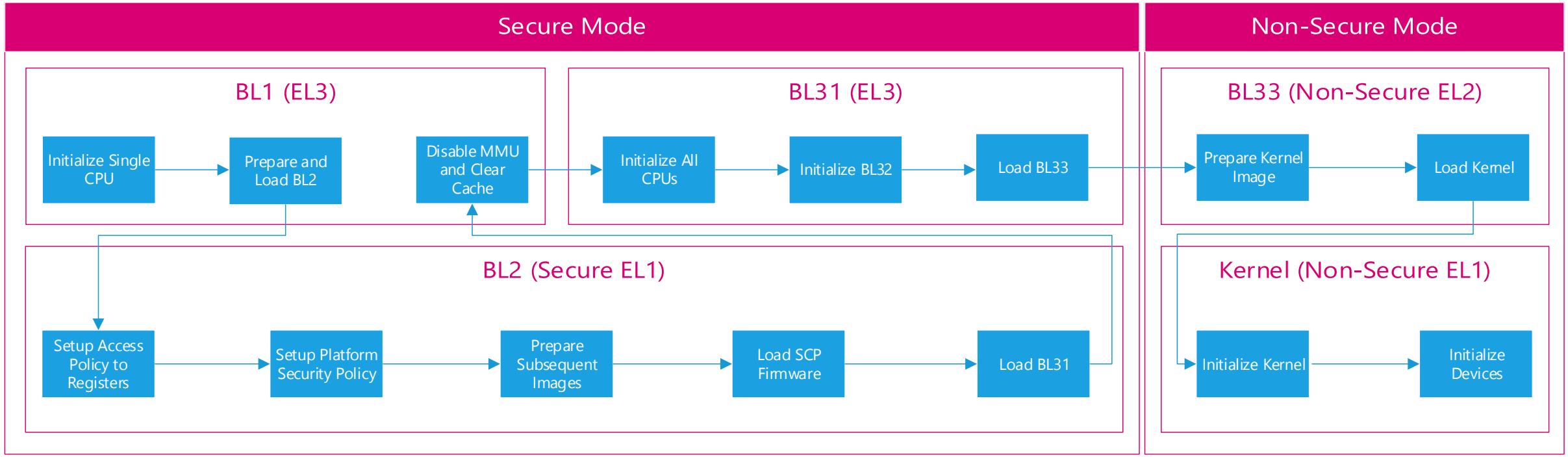
3. Dynamic Taint Analysis
   - Sensitive information leakage

- How to implement them?
  - https://fengweiz.github.io/paper/seclabel-crvf19-slides.pdf

核故障检测（Funded Industry Project）

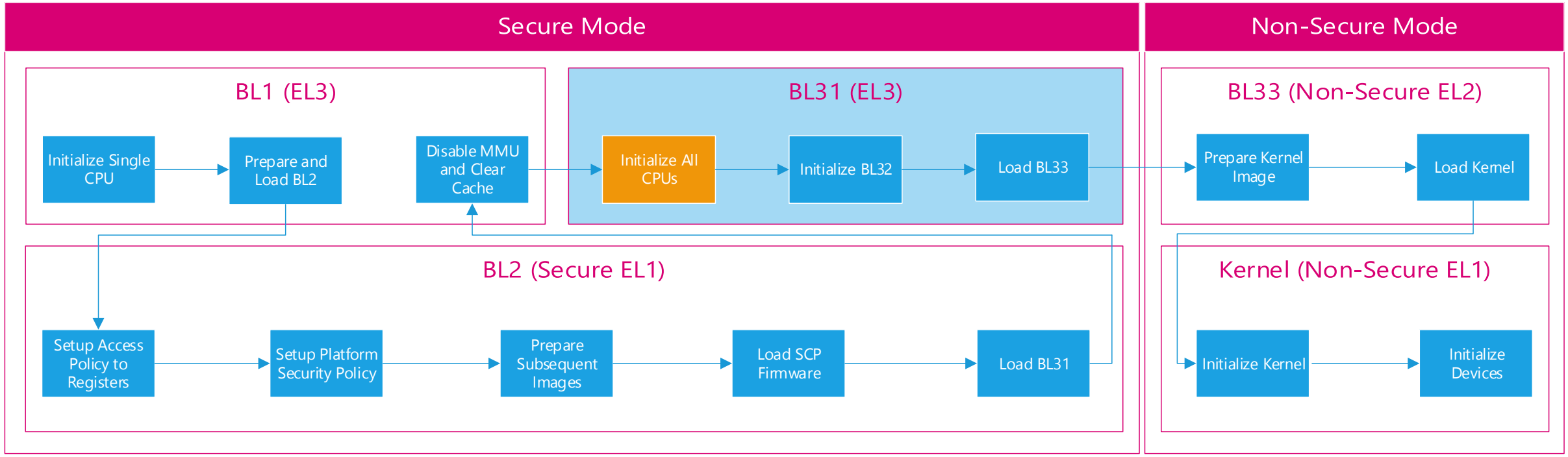
- 现有CPU在生命周期中依然存在硬件故障的可能性
  - 主要表现为CPU指令执行结果不符合预期（例如，算数指令计算错误和状态标识位错误）.
  - CPU硬件故障将直接对在该CPU上运行的程序造成不可预料的影响
- 由于CPU架构的差异，各大CPU厂商有各自的核故障检测工具.
  - 例如ARM Cortex-R和Cortex-M系列中的lock-step以及Intel BIST.

初步方案



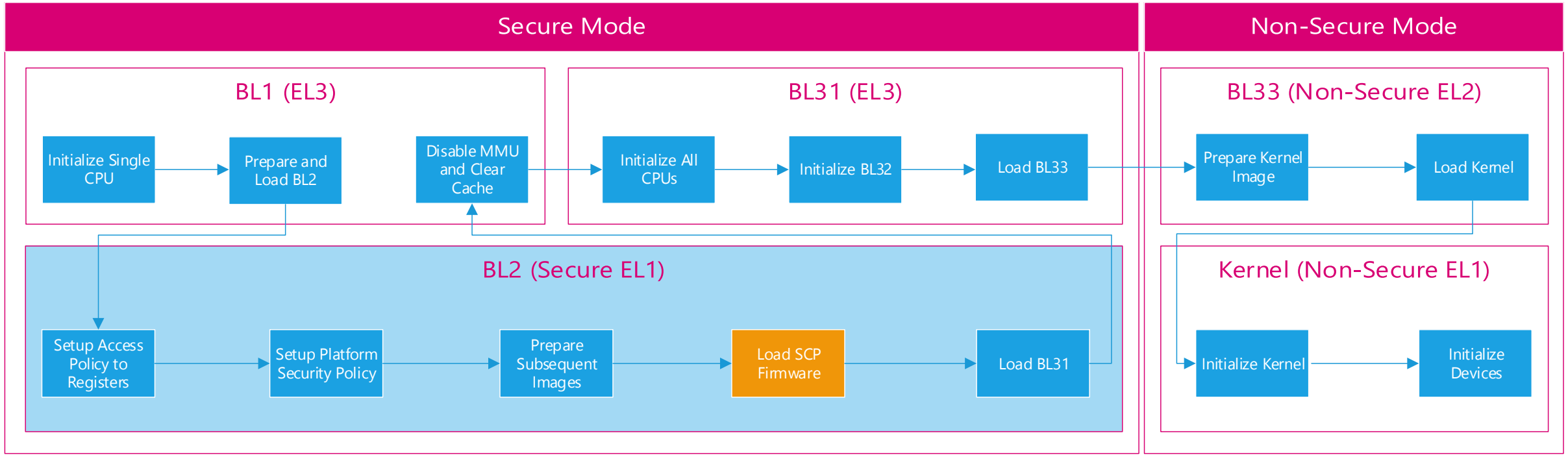
- 简化的ARM Trusted Firmware启动流程
  - 5个主要阶段，BL31前只有一个CPU在工作

初步方案



- 启动时故障检测可在BL31初始化所有CPU时完成
  - 通过多核执行相同指令并比较结果来实现故障检测

初步方案



- 运行时实时故障检测可作为协处理器固件的一部分，由协处理器来完成
  - 最小化运行时的性能损耗

钉枪（Nailgun）：Breaking Privilege Isolation on ARM

- 现更多的攻击场景
  - 云服务ARM设备，如亚马逊，阿里云等
  - 物联网设备，手机，平板电脑等
  - 拿到CVE

- 防御工作
  - 通过虚拟化的方式防止攻击者访问debugging registers，主要在EL2层实现防御代码

GPU 安全

- 现在GPU中间实现可信执行环境（TEE）

- Performance
  - Offload CPU tasks to GPU

- Security
  - Cache-based or TLB-based side channel attacks
  - CPU attacks such as Spectre and Meltdown

- ARM Mali GPU

Other Research Projects

- DexLego
  - Unpacking Android Apps
- Ninja and MalT
  - Transparent malware analysis
  - Program tracing and debugging
- Plausible Deniable Encryption

加入COMPASS

- COMPuter And System Security (COMPASS) Lab

- 创新实验课程
  - Spring 2020，Fall 2020，Spring 2021
  - 毕业设计

- 本科生勤工俭学

- RA，硕士，博士

谢谢大家！

校园里面碰到，不要装着不认识！