Securing Embedded and IoT Systems with SPMP-based Virtualization

Sandro Pinto José Martins Manuel Rodríguez Tilen Nedanovski* Ziga Putrle* Matjaz Breskvar*

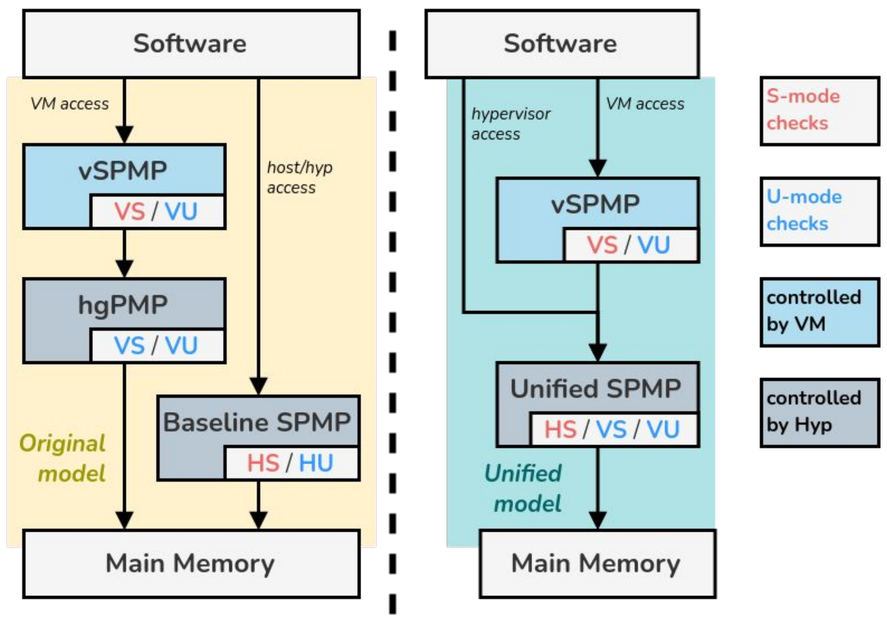
Centro ALGORITMI/LASI - Universidade do Minho, Beyond Semiconductor*

Abstract

Internet of Things (IoT) devices, typically based on low-cost microcontrollers (MCUs), are being deployed on a massive scale while becoming increasingly complex. Virtualization is the de facto solution to secure these systems, but it has not been available on MCUs until now. This paper proposes a virtualization-based Trusted Execution Environment (TEE) architecture leveraging the RISC-V Hypervisor and SPMP extensions. We have implemented a working prototype running the open-source Bao Hypervisor on top of Beyond's BA51 CPU.

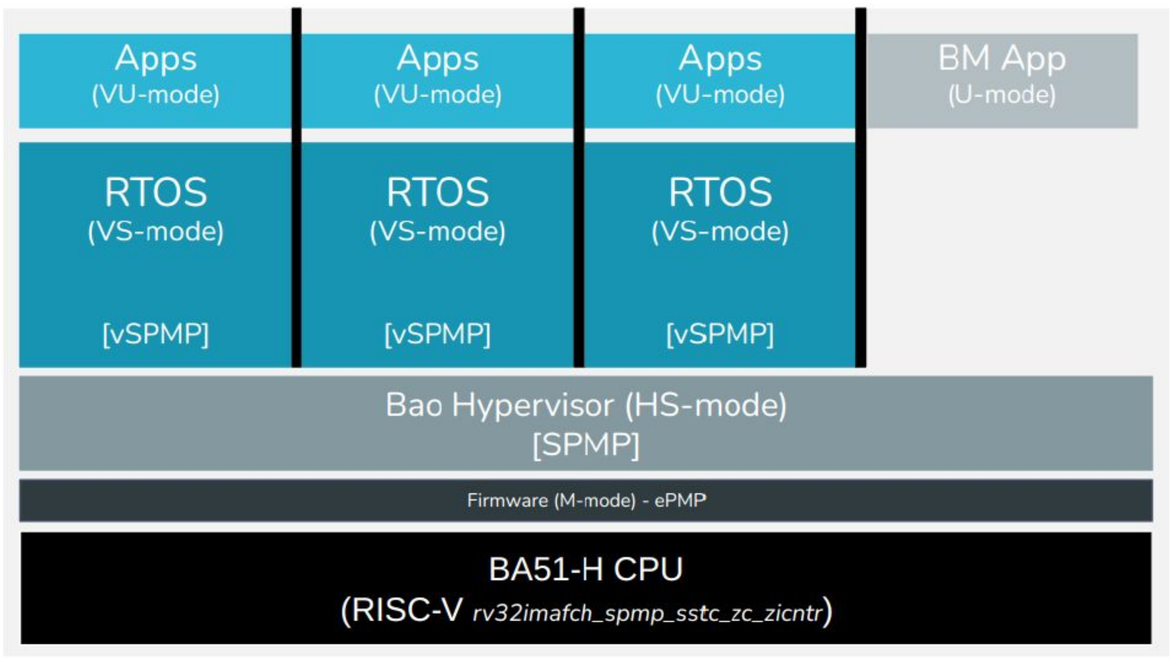
RISC-V Supervisor Physical Memory Protection (SPMP)

- Provides memory isolation for MMU-less processors
  - Between S-mode OSes (e.g., RTOS) and U-mode applications
- First SPMP extension for Hypervisor proposal -> **Dual-stage SPMP**
  - vSPMP: Controlled by VMs (VS), mediates VU accesses
  - hgPMP: Controlled by Hypervisor (HS), mediates VS/VU accesses
  - Baseline SPMP: Controlled by Hypervisor (HS), mediates HS/HU accesses
- Our proposal -> Single SPMP under Hypervisor control (**Unified model**)
  - Unifies hgPMP and baseline SPMP under the control of HS
  - VM accesses (VS/VU) are interpreted as U-mode accesses
  - Reduces the waste of possibly unused entries



System Architecture

- SPMP-based virtualization as a basis for hardware-enforced software-defined virtualization-based TEEs
- Beyond's BA51-H MCU
  - First RISC-V MCU with Hypervisor and Sspmp extensions
  - Unified SPMP model
- Bao hypervisor
  - First hypervisor running on a virtualization-ready, SPMP-based RISC-V processor
  - Fully isolated VMs as software-defined TEEs
- Target applications
  - Secure AI, Automotive (e.g., zonal controllers)



Preliminary Evaluation

A. Bao's config for the BA51-H has a total of 29.5 kiB of code size
B. Hardware extensions and (S)PMP area is offset by reduced SRAM and flexibility improvements
C. Delegation & Zc instructions are net area gain due to code size savings
D. PMP is the main area contributor for all configs
   - 1600 gates per entry for (S)PMP

Hardware Logic	Gates	Area % of (#1)	Area % of (#2)	Area % of (#3)	Area % of (#4)	
(#1) BA51 CC	25239	100%	5%	12%	3%	
(#2) BA51 CC + 64 kiB SRAM	549527	2177%	100%	266%	75%	
(#3) BA51 FRC	206430	818%	38%	100%	28%	
(#4) BA51 FRC + 64 kiB SRAM	730718	2895%	133%	354%	100%	
Hypervisor extension	7685	30.4%	B 1.4%	3.7%	B 1.1%	
PMP (16e) + unified SPMP (16e)	51223	203%	9.3%	24.8%	7%	D
PMP (32e)	50733	201%	9.2%	24.6%	6.9%	
APLIC	1403	5.6%	0.3%	0.7%	0.2%	C
Sstc	904	3.6%	0.2%	0.4%	0.1%	
Zc	1287	5.1%	0.2%	0.6%	0.2%	

Universidade do Minho OSY technologies CROSSCON BEYOND SEMICONDUCTOR