An overview of available and upcoming RISC-V security mechanisms, and their potential use in Satellite as a Service scenarios

Nick Kossifidis (FORTH), George Christou (Technical University of Crete), Manolis Surligas (Libre Space Foundation)

Introduction

Satellite-as-a-Service (SaaS) enables satellite operators to allocate computing and instrumental resources to multiple users, similar to cloud computing. This shared model introduces significant security challenges, requiring strong isolation, confidentiality, and integrity guarantees. RISC-V security mechanisms provide a robust framework to address these issues in such environments.

Threat Model

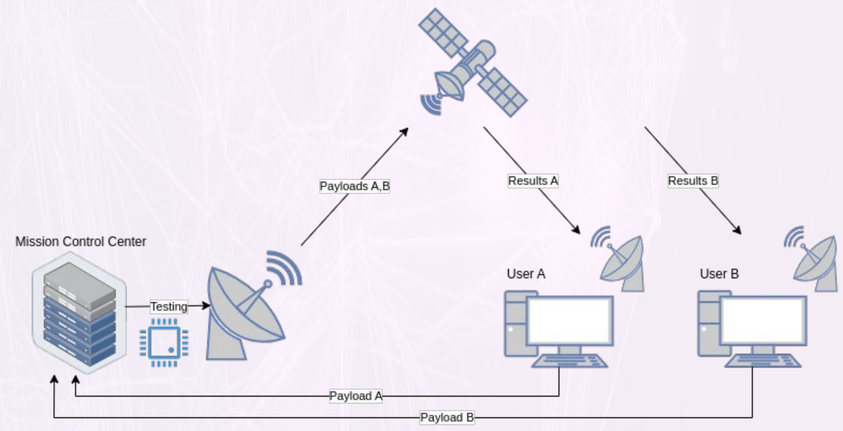
- **Shared resources introduce security risks**, including malicious user payloads targeting other users, the satellite itself, or the operator's infrastructure.
- **Confidentiality and integrity concerns** arise when workloads run in untrusted environments.
- **Security must be enforced at multiple levels:** Protecting users from each other, the operator from users, and users from the operator.
- **Continuous security monitoring** is necessary to maintain system resilience in the harsh space environment.

Mechanism	Purpose
MTE (Memory Tagging Extension)	Detects and prevents buffer overflows and use-after-free vulnerabilities
CFI (Control flow integrity)	Ensures that a program executes along intended paths, by enforcing valid control-flow transfers.
HFI (Hardware Fault Injection Protection)	Isolates untrusted process segments to prevent intra-workload interference
CHERI (Capability Hardware Enhanced RISC Instructions)	Provides fine-grained memory safety and access control
RERI (RAS Error-Record Register Interface)	Reports hardware errors for adaptive system recovery
CBQRI (Capacity & Bandwidth QoS Register Interface)	Ensures workload availability and resource allocation

Mechanism	Function	Protection Level
ePMP (Enhanced Physical Memory Protection)	Restricts access to physical memory regions / resources	CPU-side static isolation
MTT (Memory Tracking Table)	Restricts access to resources based on supervisor domain ID	CPU-side dynamic isolation
MMU (Memory Management Unit)	Enforces process separation through virtual memory	CPU-side virtual memory isolation
I/O PMP (I/O Physical Memory Protection)	Restricts physical memory access for peripherals, based on source ID	Platform-level static isolation
I/O MTT (I/O Memory Tracking Table)	Restricts physical memory access for peripherals based on supervisor domain ID	Platform-level dynamic isolation
I/O MMU (I/O Memory Management Unit)	Enforces resource separation through virtual memory	Platform-level virtual memory isolation

Integrity and Reliability Mechanisms

- **Runtime integrity is critical**, corrupted data or control-flow can spread across workloads, causing failures or security breaches.
- **Reliability is also critical** due to the extreme environment, radiation exposure, and hardware constraints.
- **Long mission duration** require fault-tolerant computing to ensure continuous operation.
- **Error detection and mitigation mechanisms** help maintain system health and extend mission longevity.



Conclusion

- RISC-V provides a **comprehensive security framework** for Satellite-as-a-Service models.
- **Memory isolation, workload separation, and integrity mechanisms** ensure robust security in space environments.
- Open RISC-V standards enable **modular, scalable, and verifiable** satellite computing platforms.
- Adoption of these mechanisms fosters **security, reliability, and innovation** in satellite-based computing.

libre.space www.higher-project.eu www.secopera.eu

HIGHER: European Heterogeneous Cloud/Edge Infrastructures for Next Generation Hybrid Services
Grant Agreement: 101189612, DG/Agency: HaDEA
Start/end date: 01.01.2025 - 31.12.2027

SecOPERA: Secure OPen source softwarE and hardwaRe Adaptable framework.
Grant Agreement: 101070599, DG/Agency: Horizon Europe
Start/end date: 01.01.2023 - 31.12.2025

European Commission

RISC-V in Space Workshop 2025
April 2 - 5, 2025