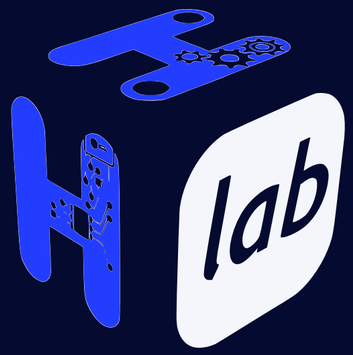

Sentry kernel key concepts

A SECURE KERNEL FOR MICRO-CONTROLERS

PART 3: DOMAIN SCHEDULING

Introduction

- **Domain scheduling concept**
  - task sets may match different usage or safety/security-related usages
  - Yet being executed on a same kernel, such as sentry, they belong to different *domains*
- **Domain scheduling goals**
  - Domain partitioning policy: inter-domain exchanges restricted (MILS concept) or filtered (MLS concept)
  - Domain ressource partitioning policy (per-domain core-load support)
  - Ensures differentiated task sets trust level, under the control of a separation kernel

domains support in Sentry

- **Sentry defines a per-task fixed domain identifier**
  - configure at project compile time for each task
  - Associated to an inter-domain policy
    - by now, inter-domain task exchanges are forbidden
    - MLS, with inter-domain gateway is considered for future releases
- **Why ?**
  - With continuous increase of micro-controllers performances & security, MILS/MLS concept is now eligible to such architectures
  - MCU-based security and safety domains separation kernel now meets real-word use cases

Domain usage examples

- **Dedicated domain for security functions**
  - A usual constraint when hardening safety-critical code is to demonstrate innocuousness of security functions
  - MILS ensures strictly partitioned security control domain that enables such a demonstration
- **Multi-IO independent domains**
  - Allows strict partitioning of two or more functions interacting with separated interfaces sets on a single MCU
- **MLS gateway**
  - Increase demonstrability of multi-level security architectures with a reduced Trusted Computing Base

Sentry MILS/MLS roadmap

- **Hierarchical scheduling**
  - Sentry scheduler is made to allow easy integration of hierarchical scheduling schemes
    - first target: TDM/RRMQ hierarchical support
      - domains time division multiplexing
      - intra-domain tasks RRMQ scheduling
  - Inter-domain hardening
    - cache cleaning, per-domain IRQ mask
      - only current domain related events are allowed
  - Easy to use integration-time time frame definition tooling to be defined

Thank you !

https://github.com/camelot-os/sentry-kernel
https://sentry-kernel.readthedocs.io/en/latest/index.html