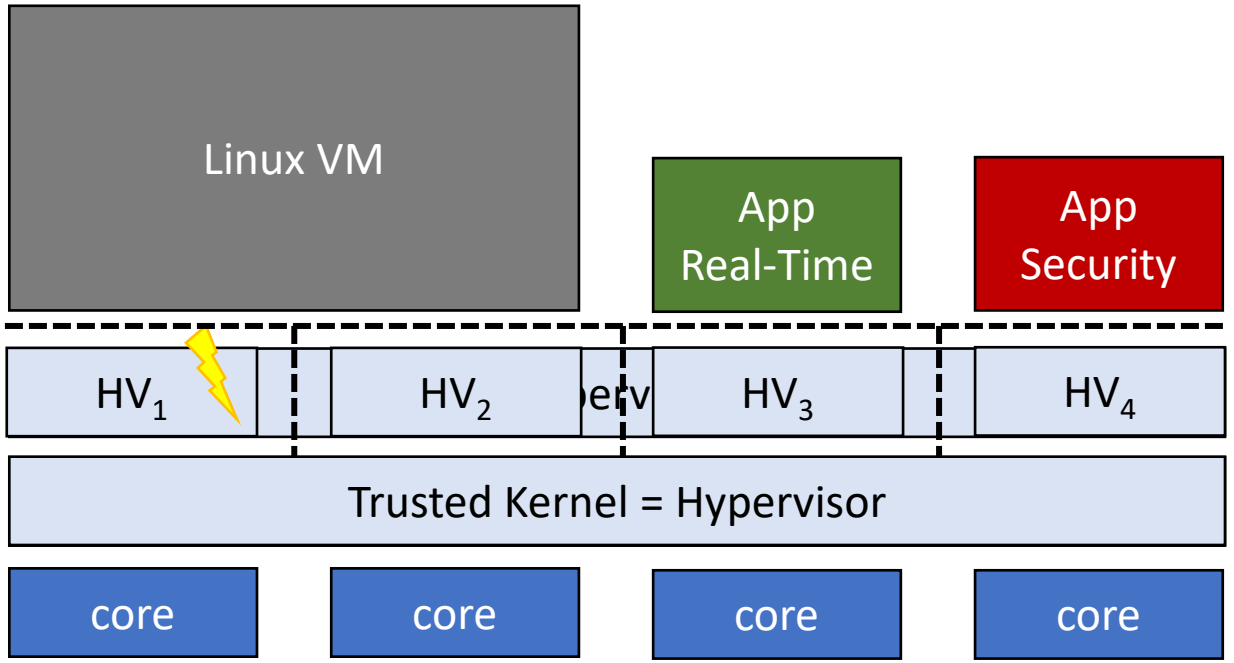
Midir: Towards Resilient SoCs

Inês Pinto Gouveia (ines.pinto.gouveia@intel.com)
Marcus Völp (marcus.voelp@uni.lu)
Paulo Esteves-Veríssimo (paulo.verissimo@kaust.edu.sa)

Behind the last line of defense: Surviving SoC faults and intrusions, Computers & Security Volume 123, December 2022, 102920

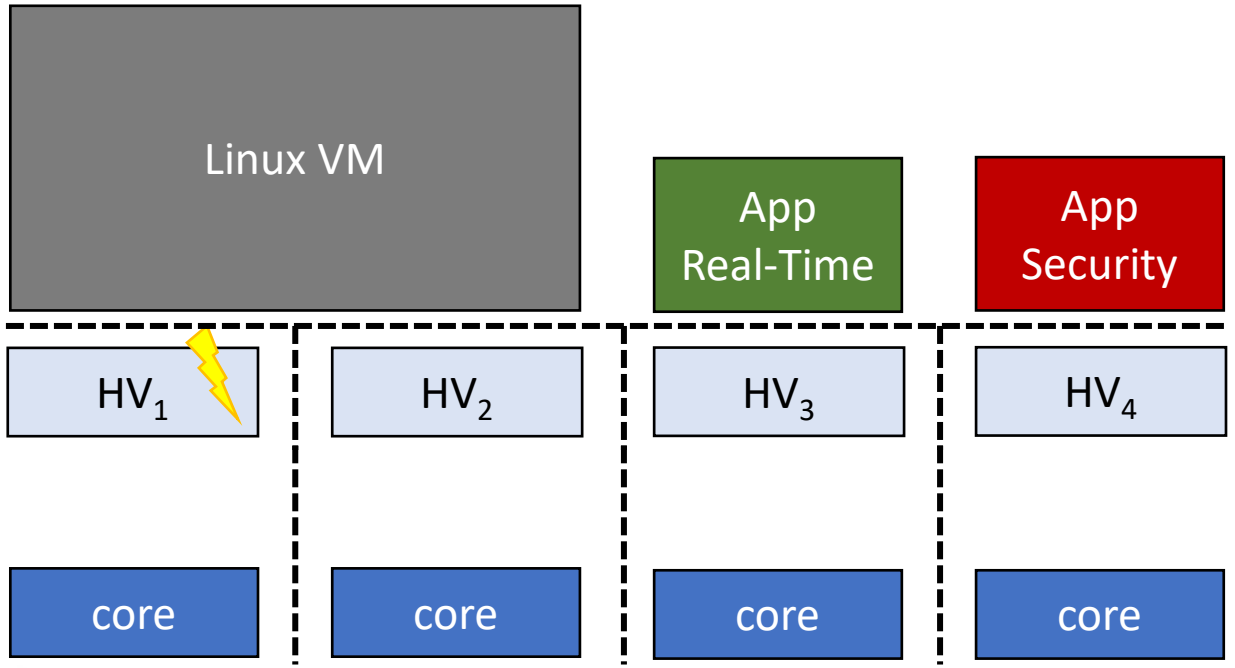
UNIVERSITY OF LUXEMBOURG

... or the story how a compromised kernel pulls himself out of the swamp



Shen Y; Heiser G; Elphinstone K, 2019, 'Fault Tolerance Through Redundant Execution on COTS Multicores: Exploring Trade-Offs', in Proceedings - 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2019, pp. 188 - 200, http://dx.doi.org/10.1109/DSN.2019.00031

... or the story how a compromised kernel pulls himself out of the swamp



Shen Y; Heiser G; Elphinstone K, 2019, 'Fault Tolerance Through Redundant Execution on COTS Multicores: Exploring Trade-Offs', in Proceedings - 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2019, pp. 188 - 200, http://dx.doi.org/10.1109/DSN.2019.00031

A slightly different setting

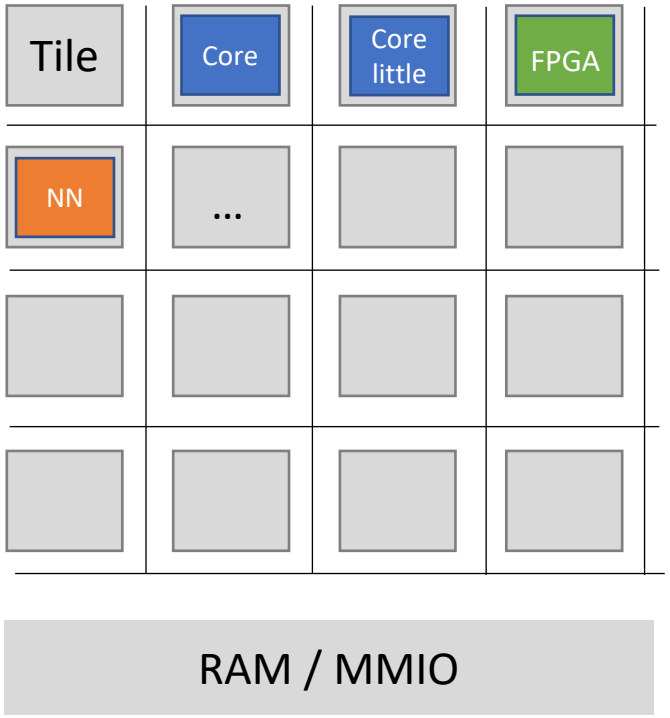
- **Hybrid system setting also for the MPSoC hardware**
  - Trusted functionality should be implemented by small and simple hardware
  - Complexity of executing instructions vs. fixed function device

=> tolerate some more hardware failures

- **Many more and diverse cores, accelerators, processing units**

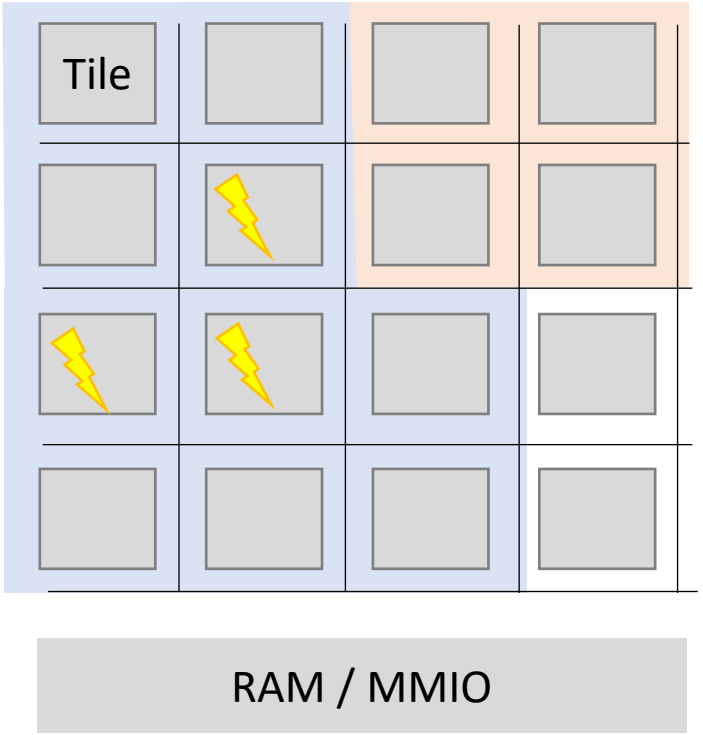
=> heterogeneous manycore SoC

- **Reliable NoC**
  (worry about that later)



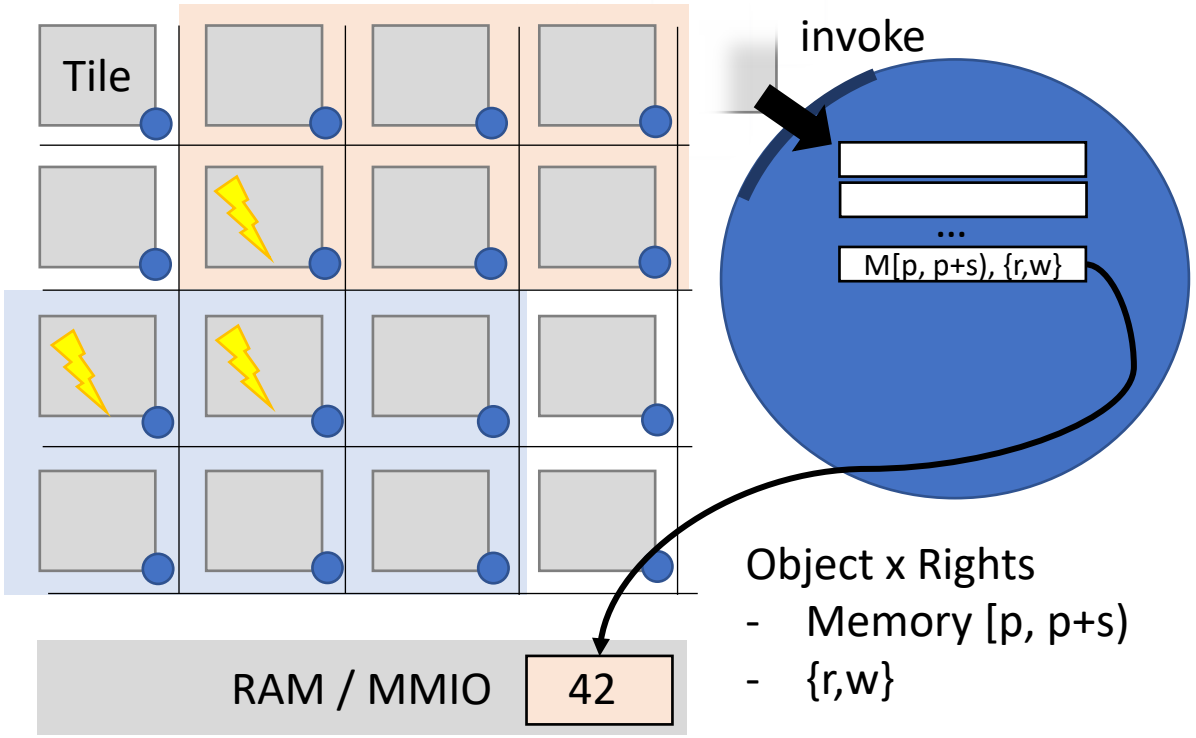
A slightly different setting

- **Dynamic Systems**
- **Fault Containment**



Midir

- Some form of privilege check
  - tile-to-RAM but also tile-to-tile
  - below and orthogonal to existing mechanisms
    - no need to handle page faults, virtualization, …
      => correct software on the tile can do that
    - confine what a tile can to (confinement boundary) not individual apps
      => updates are less frequent than PTE updates
  - we used capabilities, but it works equally well with page tables, …



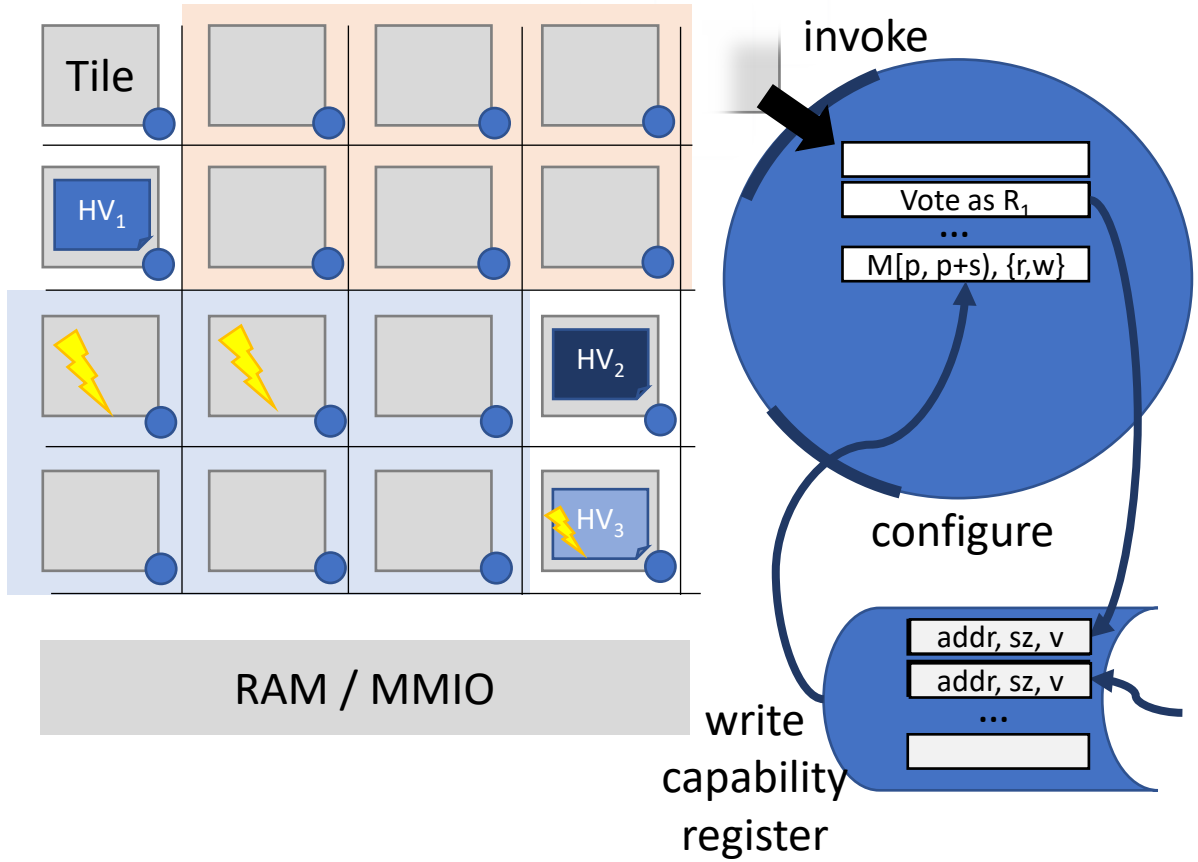
Midir

- Control / Change Privileges
  - install / remove capability
  - write page-table entry
- Consensual Privilege Change
  - for application cores (e.g., running the VMs)
  - for the hypervisor itself

  => rejuvenation

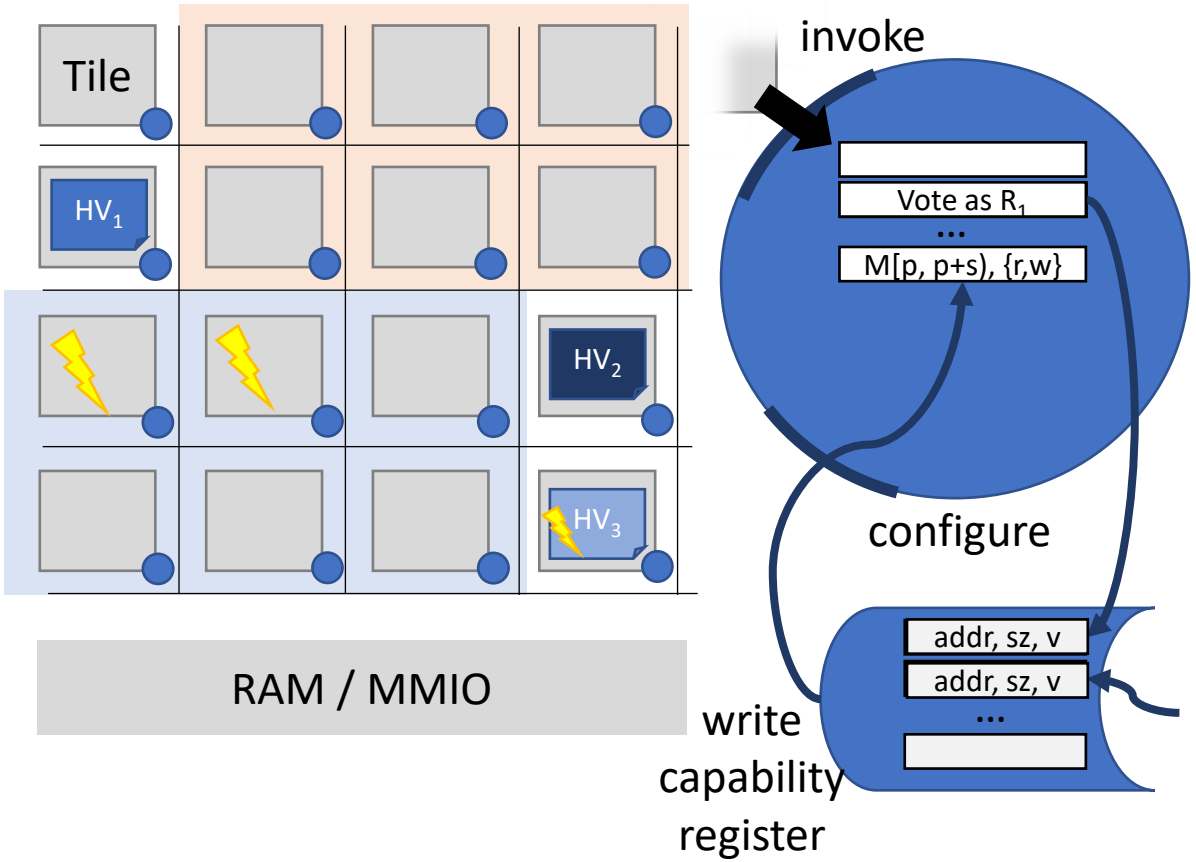
  => relocation

  => privilege reversion



Midir

- Conclusion and Future Work
  - SoC-level resilience also works for dynamic systems
  - Tolerate large class of hardware faults (those that are contained to a tile and its outputs)
  - Further explore privilege reversion
  - Partial dynamic reconfiguration of FPGAs to rejuvenate hardware
  - …



@PhD students:
don't hesitate asking any of the WG participants for internships / postdoc positions / …