Design of a secured kernel for constrained objects

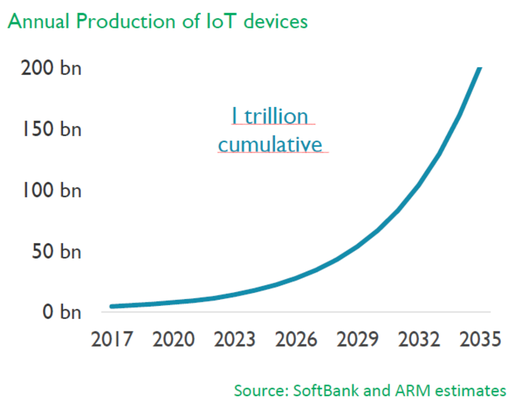
16/12/2020

RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information) 2020

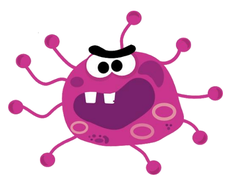
PhD student: Nicolas Dejon ; Industrial advisor: Chrystel Gaber, PhD ; Supervisor: Prof. Gilles Grimaud

IoT devices need security

IoT in expansion



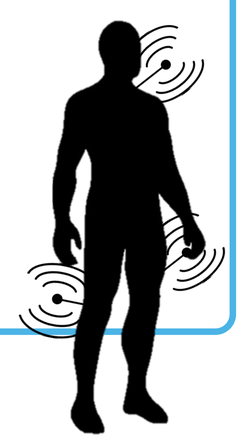
Increased cyberattacks and impacts



Mirai, Stuxnet,
hacked Jeep Cherokee,
hacked coffee machine

IoT device's constrained resources

- Less memory
- Less computing power
- Very heterogeneous devices



Isolation, a means for security-by-design

stronger isolation guarantees

Tiny embedded systems FreeRTOS RIOT OS Zephyr	TockOS, Zephyr (MPU), RIOT-OS (MPU), MbedOS, Choupi-OS, TrustedFirmware-M, FreeRTOS-MPU MINION, ACES, TrustLite	EwoK (WooKey)	ProvenCore-M
General-purpose systems/ High-end embedded systems Linux TrustedFirmware-A Fuchsia		Pip + OS seL4	
No HW protection	HW protection (MMU, MPU, TrustZone…)		

Proprietary/ limited information

Open innovation Open-source

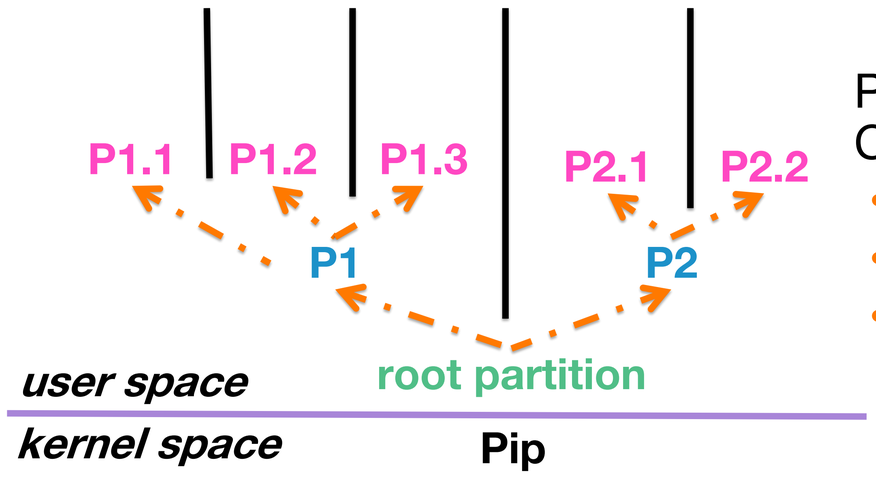
Minimalist by design

Provide **strong isolation guarantees** by being at least
- **– hardware-based** AND
- – ensured by **formal proofs** AND

- fits **constrained devices** AND
- is **open-source**

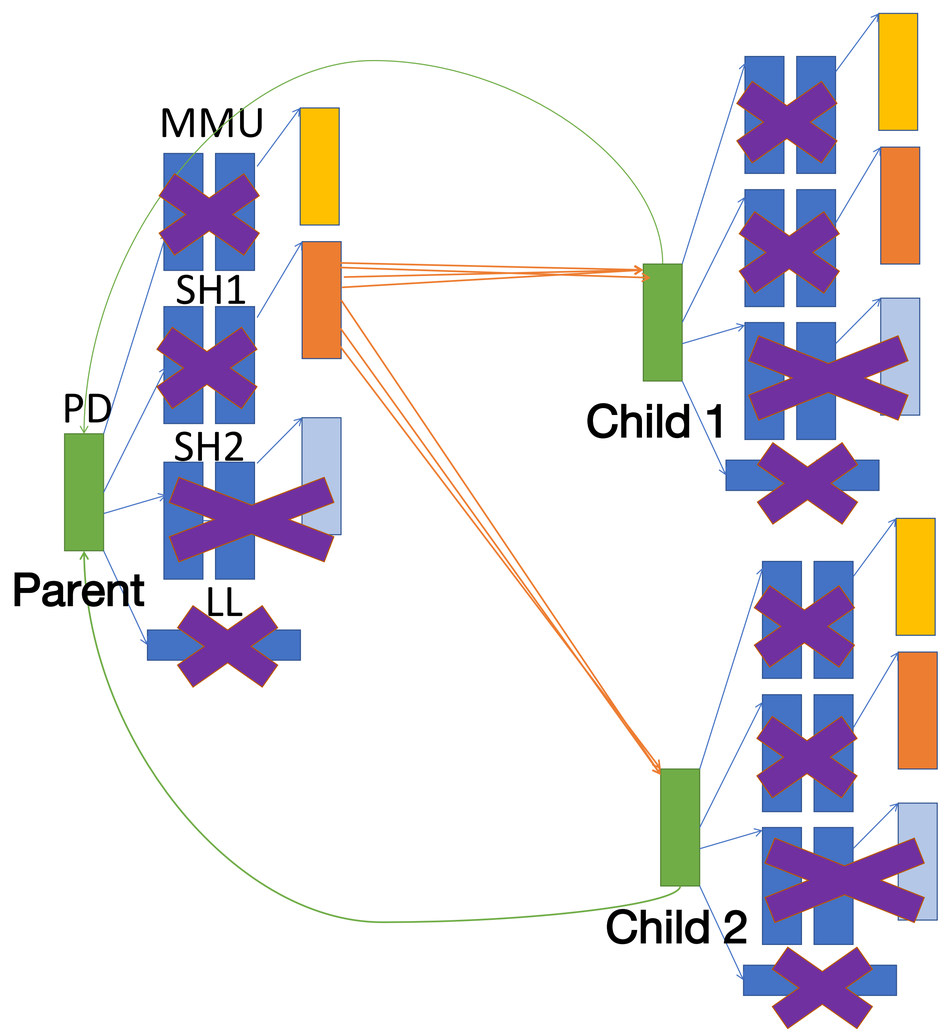
Adapting the Pip protokernel for constrained IoTs

Pip



Properties proved in the Coq Proof Assistant:
- **horizontal isolation**
- **vertical sharing**
- **kernel isolation**

Optimizing & transitioning from Pip-MMU to Pip-MPU, Impacts on partition metadata



Challenges

- Pip's flexibility
- Adapt the formal proofs
- Reach the lowest possible assumptions
- Maintain ease of adoption, broad use cases