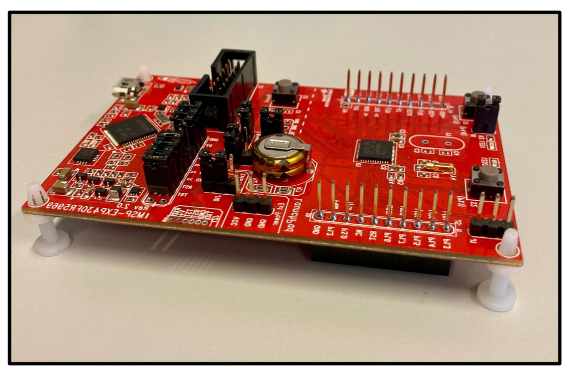
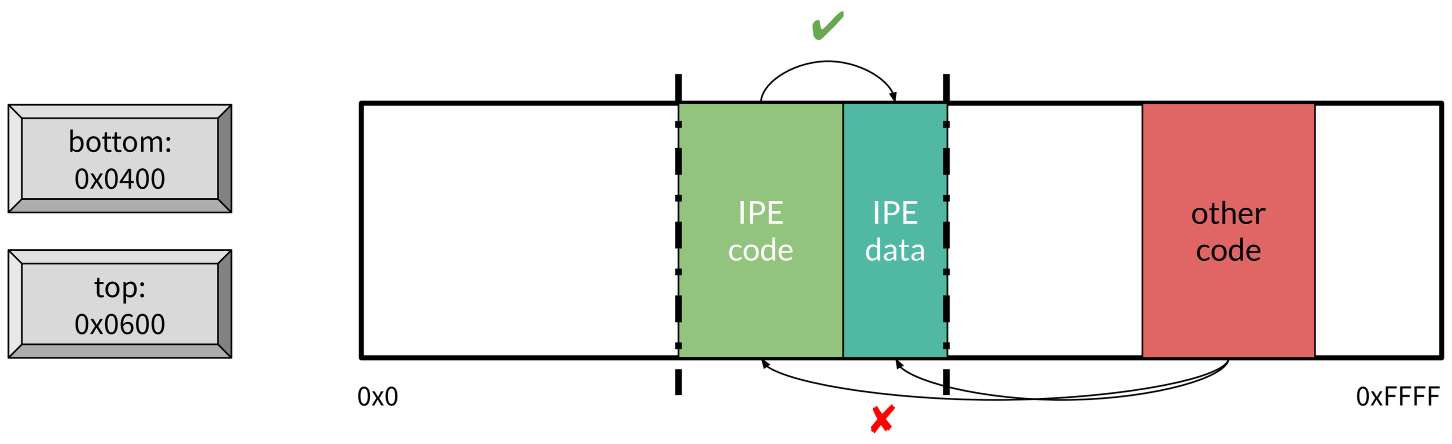
openIPE: An Extensible Memory Isolation Framework for Microcontrollers

Marton Bognar, Jo Van Bulck
DistriNet, KU Leuven, Belgium
marton.bognar@kuleuven.be
jo.vanbulck@kuleuven.be

Texas Instruments IPE

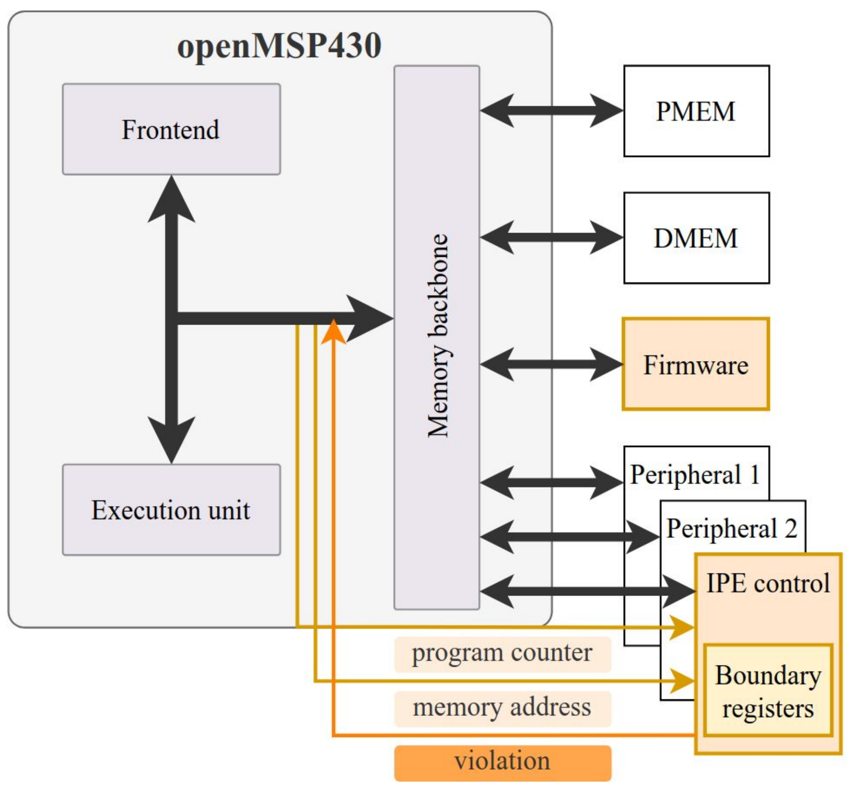
- MSP430: Low-power microcontrollers
- FRAM edition (2014) with security features:
  - Physical tamper protection
  - Hardware AES cryptographic unit
  - Memory protection unit (MPU)
  - **Intellectual Property Encapsulation (IPE)**





The openIPE architecture

Goal: extensible IPE-compatible **memory isolation** with a flexible trusted firmware layer



Access control matrix

From \ To	Untrusted	Firmware	IPE	IPE entry
Untrusted	rwx	r--	---	--x
Firmware	rxw	rwx	rwx	rwx
IPE + entry	rwx	r--	rwx	rwx
DMA	rw-	r--	---	---
Debug unit	rw-	r--	---	---

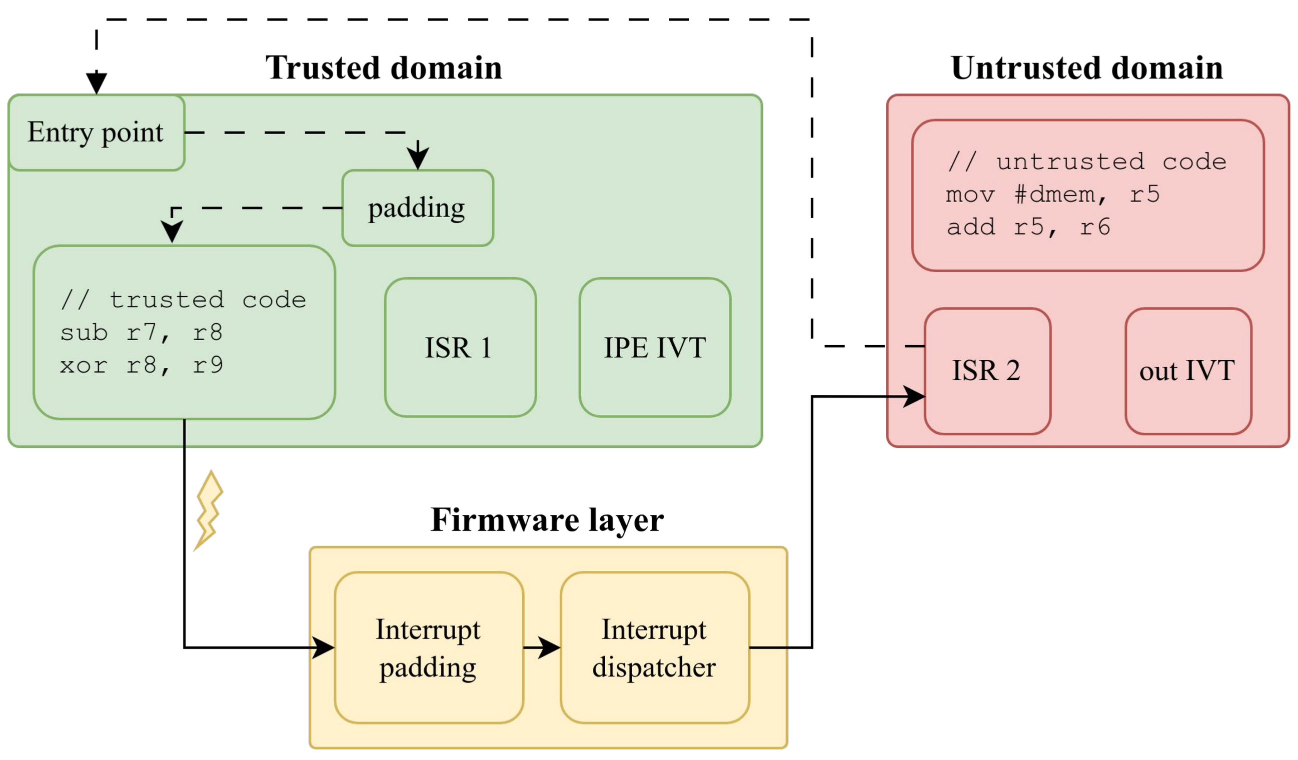
Hardware cost

Design	LUTs	Δ LUTs	FFs	Δ FFs
openMSP430 (baseline)	2,311	-	1,110	-
IPE specification	2,510	+8.6%	1,162	+4.7%
openIPE	2,582	+11.7%	1,191	+7.3%

Case study: Secure interrupts

Approach	Secure scheduling	Architectural protection	Interrupt latency mitigation	Untrusted interrupts
Software disable	○	◐	●	○
Hardware disable	○	●	●	○
SW-IRQ (de Clercq, 2014)	◐	●	○	●
FW-IRQ *(our proposal)*	◐	●	●	●

FW-IRQ using the trusted firmware



- FW-IRQ offers the **strongest** guarantees
  - Software-based padding for interrupt-latency attacks
- Other hardware-based approaches are more expensive:
  - de Clercq, 2014: +186 LUTs and +34 FFs (only architectural)
  - Sancus_V: +142 LUTs and +260 FFs

Design	LUTs	FFs	Δ Software
openIPE (baseline)	2,582	1,191	–
Software disable	–	–	8 bytes / 6 cycles
Hardware disable	2,581 (-1)	1,191	–
SW-IRQ	2,597 (+15)	1,191	282 bytes / 198 cycles
FW-IRQ	2,577 (-5)	1,190 (-1)	674 bytes / 417 cycles

MSP430 in research

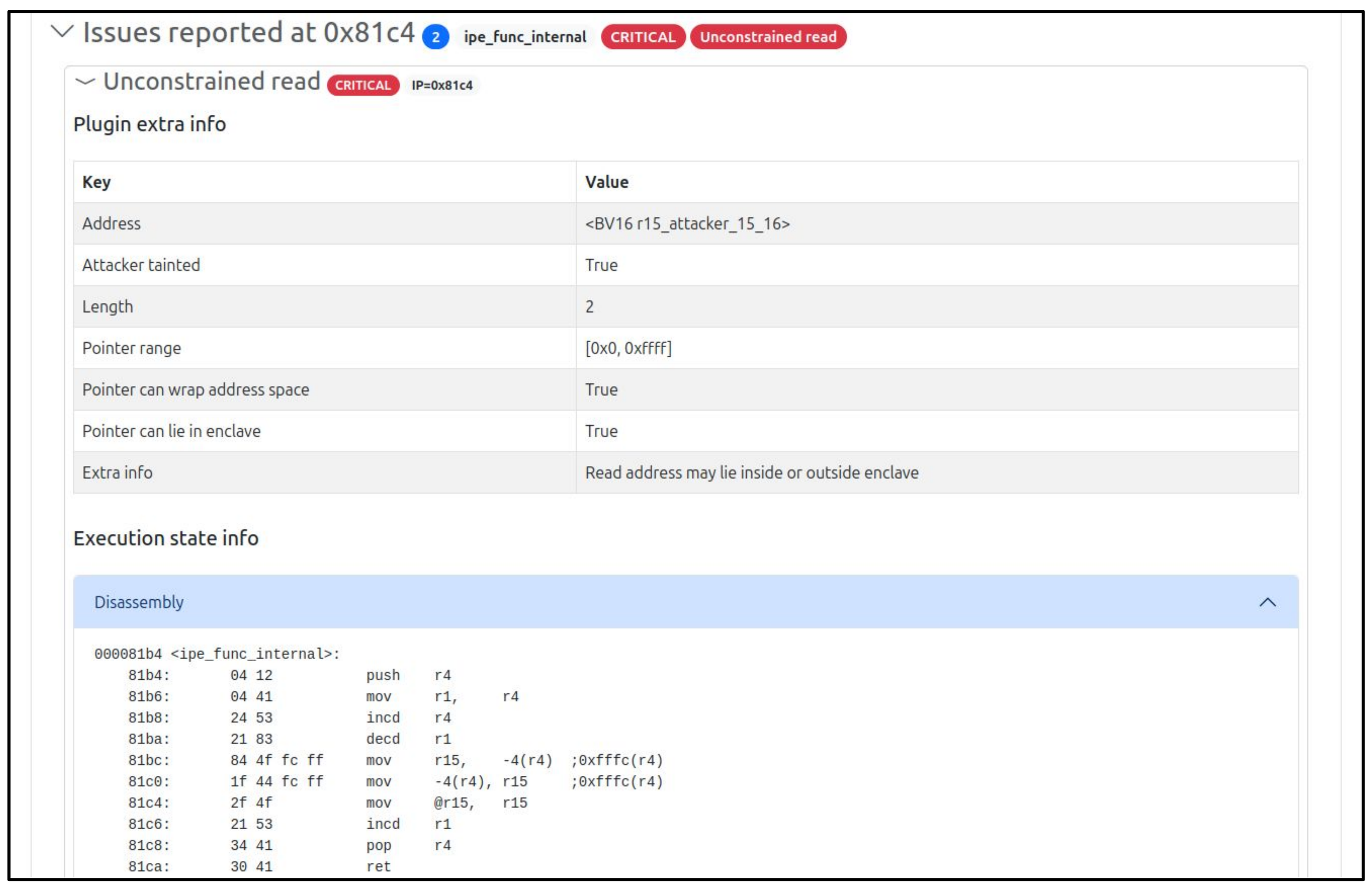
	name	year	venue	code	data	dyn.	extension	untr. ISR	open src.	ind. spec.	attacks
openMSP430	SMART [3]	2012	NDSS	○	●	○	Hybrid	○	○	○	[4], [56], [57]
	↪ ERASMUS [58]	2018	DATE	○	●	○	Hybrid	○	○	○	–
	Sancus 1.0 [59]	2013	USENIX	○	●	●	Hardware	○	●	○	–
	↪ Soteria [60]	2015	ACSAC	●	●	●	Hardware	○	●	○	–
	↪ Towards Availability [11]	2016	MASS	○	●	●	Hardware	●	○	○	–
	↪ Sancus 2.0 [2]	2017	TOPS	●	●	●	Hardware	○	●	○	[21], [22]
	↪ Sancus_V [33]	2020	CSF	●	●	●	Hardware	●	●	○	[23], [34], [35]
	↪ Aion [8]	2021	CCS	●	●	●	Hybrid	●	●	○	–
	↪ Authentic Execution [61]	2023	TOPS	●	●	●	Hybrid	○	●	○	–
	de Clercq et al. [7]	2014	ASAP	○	●	●	Hybrid	●	○	○	–
	VRASED [4]	2019	USENIX	○	●	○	Hybrid	○	●	○	[23]
	↪ APEX [57]	2020	USENIX	○	●	○	Hybrid	○	●	○	[23]
	↪ ASAP [62]	2022	DAC	○	●	○	Hybrid	●	●	○	–
	↪ RARES [63]	2023	arXiv	○	●	○	Hybrid	○	○	○	–
	↪ RATA [64]	2021	CCS	○	●	○	Hybrid	○	●	○	–
	↪ CASU [65]	2022	ICCAD	○	●	○	Hybrid	●	●	○	–
	↪ VERSA [66]	2022	S&P	○	●	○	Hybrid	○	●	○	–
	↪ ACFA [67]	2023	USENIX	○	●	○	Hybrid	○	●	○	–
	GAROTA [68]	2022	USENIX	◐	◐	○	Hybrid	○	●	○	–
	IDA [10]	2024	NDSS	○	●	○	Hybrid	●	○	○	–
	UCCA [69]	2024	TCAD	●	●	○	Hardware	●	●	○	–
	openIPE *(this work)*	2025	EuroS&P	●	●	●	Hybrid	●	●	●	–
TI MSP430	IPE [46]	2014	–	●	●	●	Hardware	○	○	●	[19], [20]
	↪ SIA [70]	2019	HOST	●	●	●	Software	○	○	●	–
	↪ SICP [71]	2020	JHSS	○	●	●	Software	○	○	●	–
	↪ Optimized SICP [72]	2022	TECS	○	●	●	Software	○	●	●	–
	↪ IPE Exposure [19]	2024	USENIX	●	●	●	Software	○	●	●	§4.2
	Hardin et al. [73]	2018	ATC	●	●	○	Software	○	○	●	–
	PISTIS [74]	2022	USENIX	●	●	●	Software	●	●	●	–
	↪ FLAShadow [75]	2024	TIOT	●	●	●	Software	●	●	●	–

- Many architectures building on openMSP430
- Building custom memory isolation primitives
- Overlapping vulnerabilities
- Cannot prototype hardware changes on TI microcontrollers

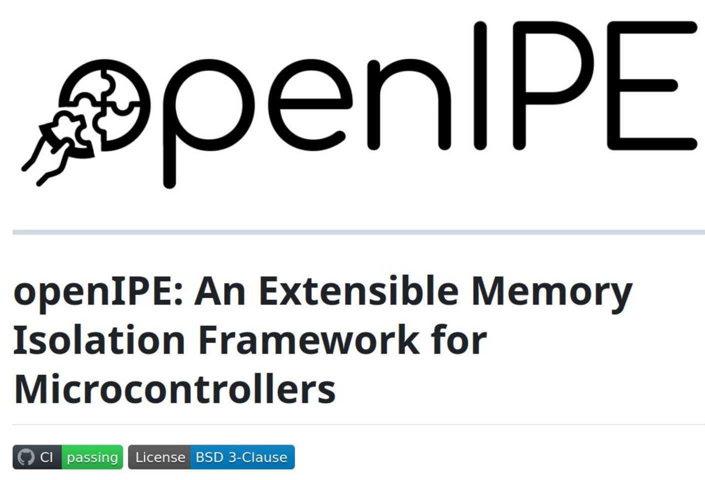
Security testing

- **Unit testing**
  - Functional and security unit tests
  - Backwards compatibility for (future) extensions
- **Symbolic execution**
  - Applied to firmware and IPE code
  - Based on Pandora (Alder, 2024)
  - Intuitive reports

# tests	Tested functionality
4	IPE boundary setup
2	Modification of boundary registers
3	Protection from untrusted code
3	Protection from the debugger
2	Protection from DMA
1	Normal access from inside the IPE region
4	Protection from known attacks
4	Protection of the firmware region
3	Case study behavior
62	openMSP430 regression tests



Resources



https://github.com/martonbognar/openipe

R. de Clercq et al., "**Secure interrupts on low-end microcontrollers**". In IEEE International Conference on Application-Specific Systems, Architectures and Processors (ASAP), 2014.
F. Alder et al., "**Pandora: Principled symbolic validation of Intel SGX enclave runtimes**". In IEEE Symposium on Security and Privacy (S&P), 2024.
M. Busi et al., "**Provably secure isolation for interruptible enclaved execution on small microprocessors**". In IEEE Computer Security Foundations Symposium (CSF), 2020.
M. Bognar et al., "**Intellectual property exposure: Subverting and securing intellectual property encapsulation in Texas Instruments microcontrollers**". In USENIX Security Symposium, 2024.

DistriNet KU LEUVEN