openIPE: An Extensible Memory Isolation Framework for Microcontrollers

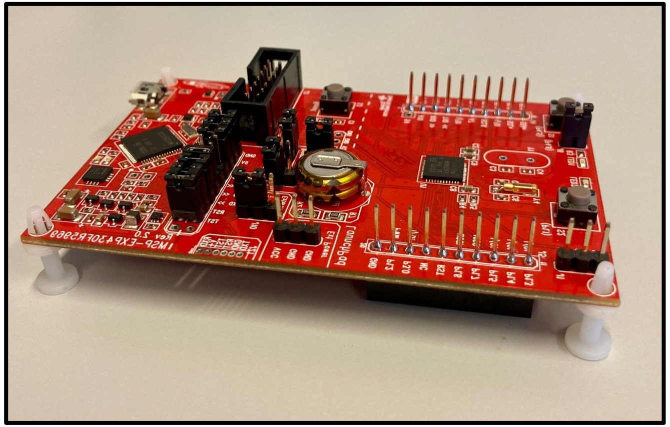
<u>Marton Bognar</u>, Jo Van Bulck
DistriNet, KU Leuven, Belgium
@ EuroS&P (July 3rd, 2025)

DistriNet

KU LEUVEN

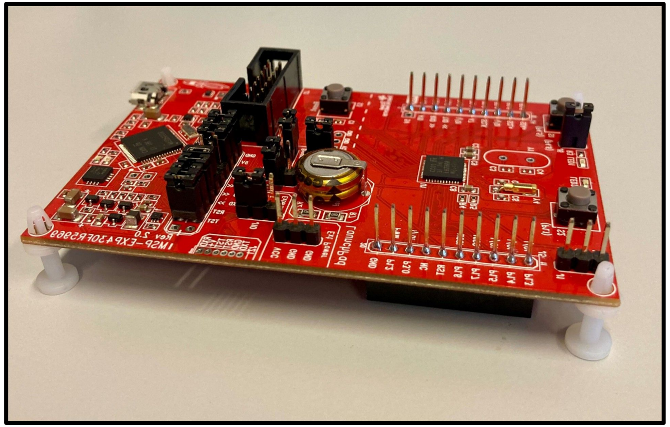
open... IPE?

Texas Instruments MSP430 microcontroller



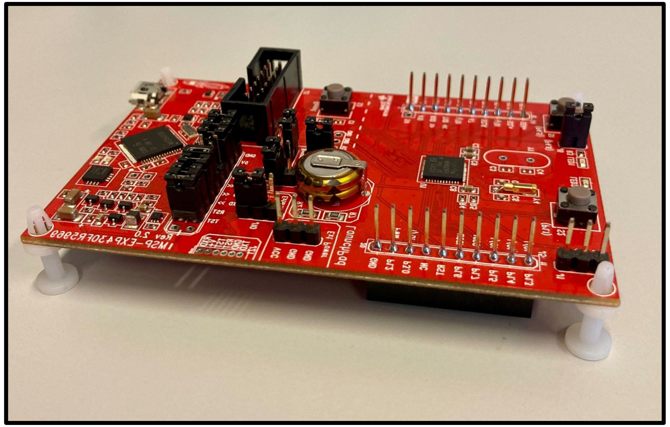
- Low-power microcontrollers

Texas Instruments MSP430 microcontroller



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

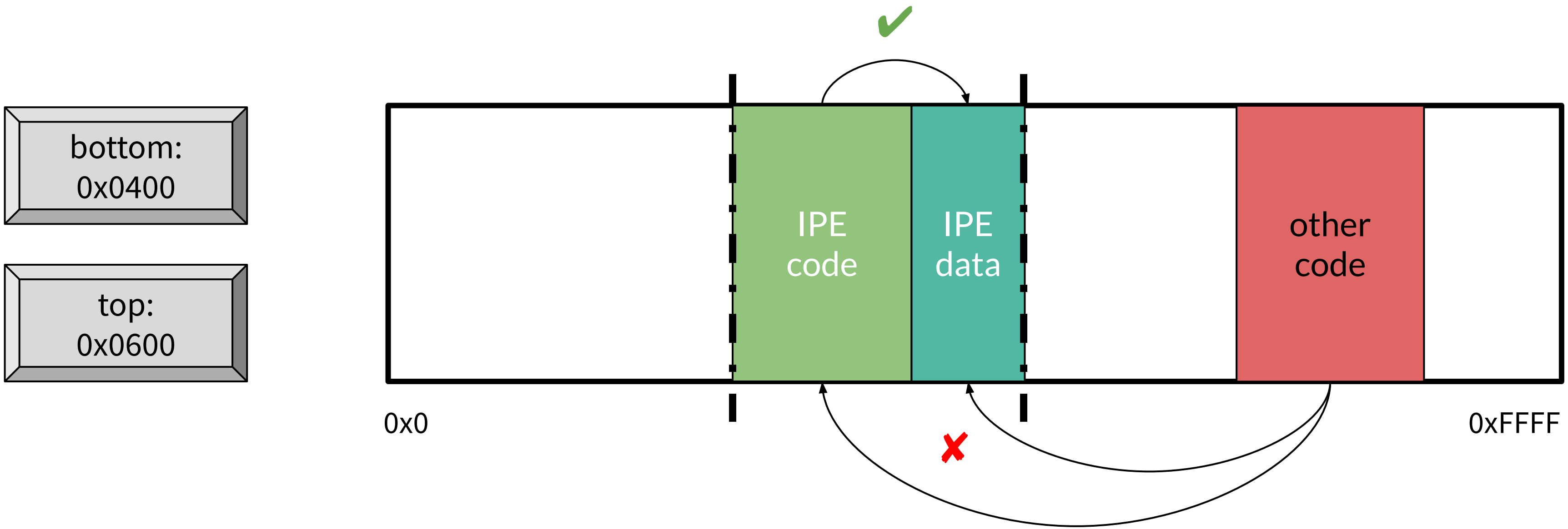
Texas Instruments MSP430 microcontroller



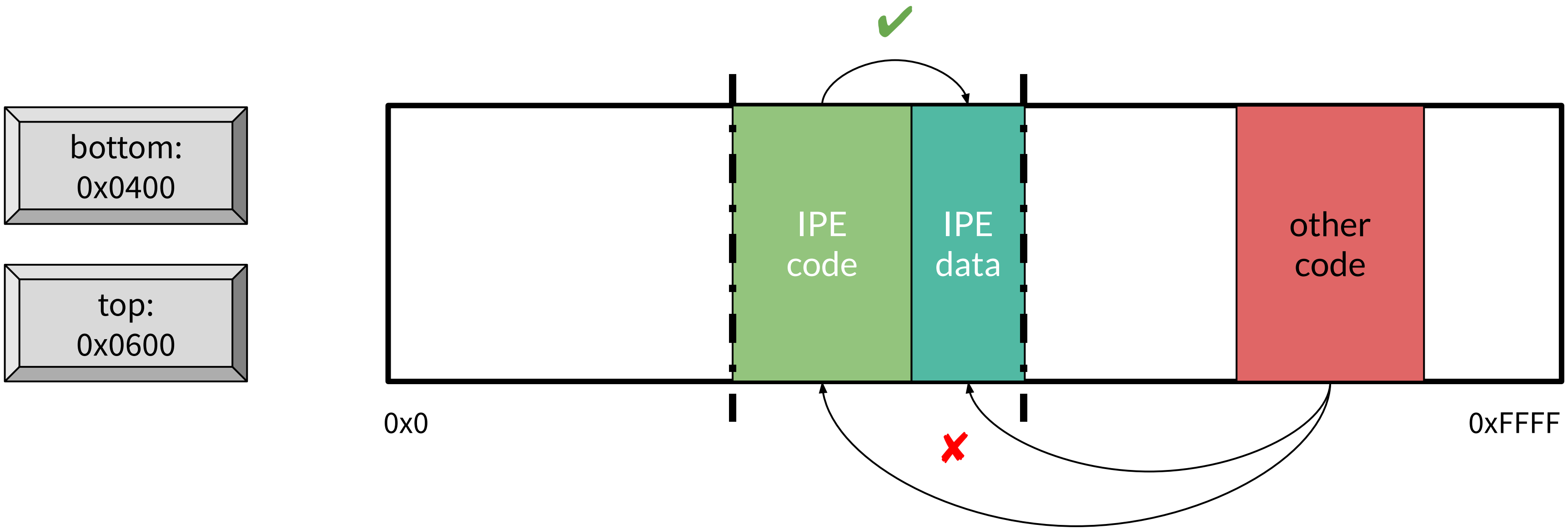
- Low-power microcontrollers
- FRAM edition (2014) with <u>security features:</u>
    - Physical tamper protection
    - Hardware AES cryptographic unit
    - Memory protection unit (MPU)
    - **Intellectual Property Encapsulation (IPE)**

"The IPE module protects a programmed portion of memory from read or write access from anywhere outside of the IP Encapsulated area, even by JTAG. This IPE module minimizes risk of exposure of critical or proprietary software from the rest of the application [...]"

Intellectual Property Encapsulation (IPE)



Intellectual Property Encapsulation (IPE)



+ protection from JTAG debug port, direct memory access (DMA)

→ Program-counter-based access control

→ **Memory isolation!**

open?... IPE

Research trends in memory isolation

- **openMSP430:** popular in research
  - Many systems (re-)implement isolation features
  - No compatibility with each other or industry standards
  - Limited applicability to real-world devices

	name	year	venue
openMSP430	SMART [3]	2012	NDSS
	↪ ERASMUS [51]	2018	DATE
	Sancus 1.0 [52]	2013	USENIX
	↪ Soteria [53]	2015	ACSAC
	↪ Towards Availability [11]	2016	MASS
	↪ Sancus 2.0 [2]	2017	TOPS
	↪ Sancus_V [33]	2020	CSF
	↪ Aion [8]	2021	CCS
	↪ Authentic Execution [54]	2023	TOPS
	de Clercq et al. [7]	2014	ASAP
	VRASED [4]	2019	USENIX
	↪ APEX [50]	2020	USENIX
	↪ ASAP [55]	2022	DAC
	↪ RARES [56]	2023	arXiv
	↪ RATA [57]	2021	CCS
	↪ CASU [58]	2022	ICCAD
	↪ VERSA [59]	2022	S&P
	↪ ACFA [60]	2023	USENIX
	GAROTA [61]	2022	USENIX
	IDA [10]	2024	NDSS
	UCCA [62]	2024	TCAD

Research trends in memory isolation

- **openMSP430:** popular in research
  - Many systems (re-)implement isolation features
  - No compatibility with each other or industry standards
  - Limited applicability to real-world devices
- **TI MSP430** difficult to do research on:
  - Closed-source hardware and firmware
  - No white-box simulator

	name	year	venue
openMSP430	SMART [3]	2012	NDSS
	↪ ERASMUS [51]	2018	DATE
	Sancus 1.0 [52]	2013	USENIX
	↪ Soteria [53]	2015	ACSAC
	↪ Towards Availability [11]	2016	MASS
	↪ Sancus 2.0 [2]	2017	TOPS
	↪ Sancus$_V$ [33]	2020	CSF
	↪ Aion [8]	2021	CCS
	↪ Authentic Execution [54]	2023	TOPS
	de Clercq et al. [7]	2014	ASAP
	VRASED [4]	2019	USENIX
	↪ APEX [50]	2020	USENIX
	↪ ASAP [55]	2022	DAC
	↪ RARES [56]	2023	arXiv
	↪ RATA [57]	2021	CCS
	↪ CASU [58]	2022	ICCAD
	↪ VERSA [59]	2022	S&P
	↪ ACFA [60]	2023	USENIX
	GAROTA [61]	2022	USENIX
	IDA [10]	2024	NDSS
	UCCA [62]	2024	TCAD
TI MSP430	IPE [39]	2014	–
	↪ SIA [63]	2019	HOST
	↪ SICP [64]	2020	JHSS
	↪ Optimized SICP [65]	2022	TECS
	↪ IPE Exposure [20]	2024	USENIX
	PISTIS [66]	2022	USENIX
	↪ FLAShadow [67]	2024	TIOT
	openIPE *(this work)*	2025	EuroS&P

Overlapping vulnerabilities

Nemesis: Studying Microarchitectural Timing Leaks in Rudimentary CPU Interrupt Logic

Jo Van Bulck
imec-DistriNet, KU Leuven
jo.vanbulck@cs.kuleuven.be

Frank Piessens
imec-DistriNet, KU Leuven
frank.piessens@cs.kuleuven.be

Raoul Strackx
imec-DistriNet, KU Leuven
raoul.strackx@cs.kuleuven.be

@CCS'18

Mind the Gap: Studying the Insecurity of Provably Secure Embedded Trusted Execution Architectures

Marton Bognar
marton.bognar@kuleuven.be
imec-DistriNet, KU Leuven
3001 Leuven, Belgium

Jo Van Bulck
jo.vanbulck@kuleuven.be
imec-DistriNet, KU Leuven
3001 Leuven, Belgium

Frank Piessens
frank.piessens@kuleuven.be
imec-DistriNet, KU Leuven
3001 Leuven, Belgium

@S&P'22

A Tale of Two Worlds: Assessing the Vulnerability of Enclave Shielding Runtimes

Jo Van Bulck
imec-DistriNet, KU Leuven
jo.vanbulck@cs.kuleuven.be

David Oswald
The University of Birmingham, UK
d.f.oswald@cs.bham.ac.uk

Eduard Marin
The University of Birmingham, UK
e.marin@cs.bham.ac.uk

Abdulla Aldoseri
The University of Birmingham, UK
axa1170@student.bham.ac.uk

Flavio D. Garcia
The University of Birmingham, UK
f.garcia@cs.bham.ac.uk

Frank Piessens
imec-DistriNet, KU Leuven
frank.piessens@cs.kuleuven.be

@CCS'19

Intellectual Property Exposure: Subverting and Securing Intellectual Property Encapsulation in Texas Instruments Microcontrollers

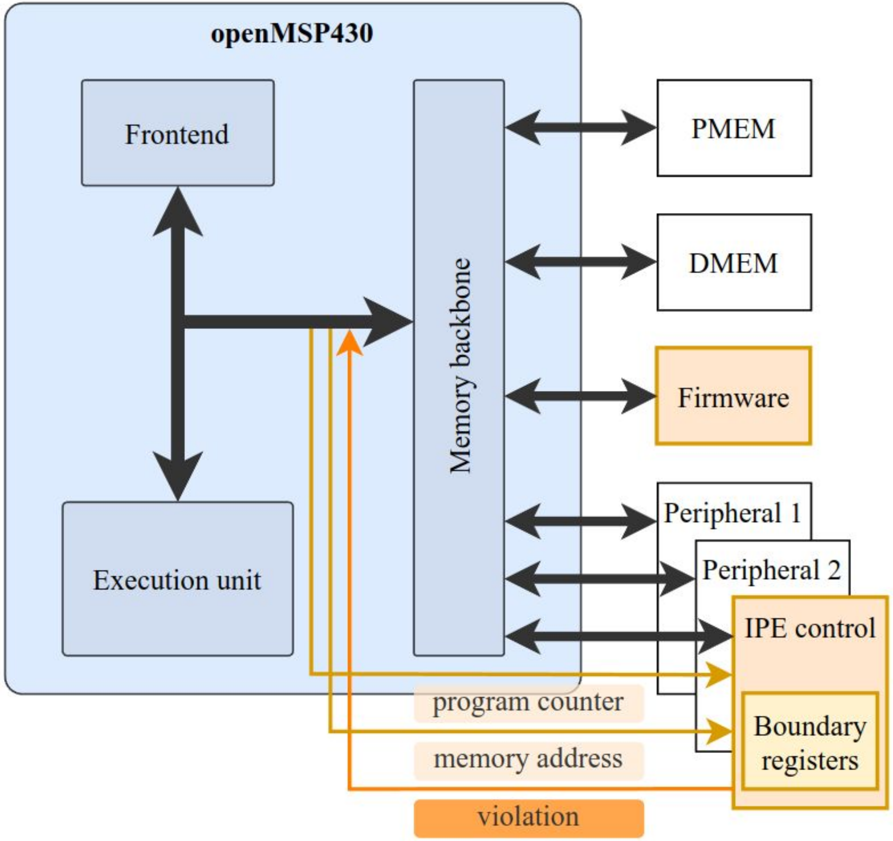
Marton Bognar, Cas Magnus, Frank Piessens, Jo Van Bulck

DistriNet, KU Leuven, 3001 Leuven, Belgium

@USENIX'24

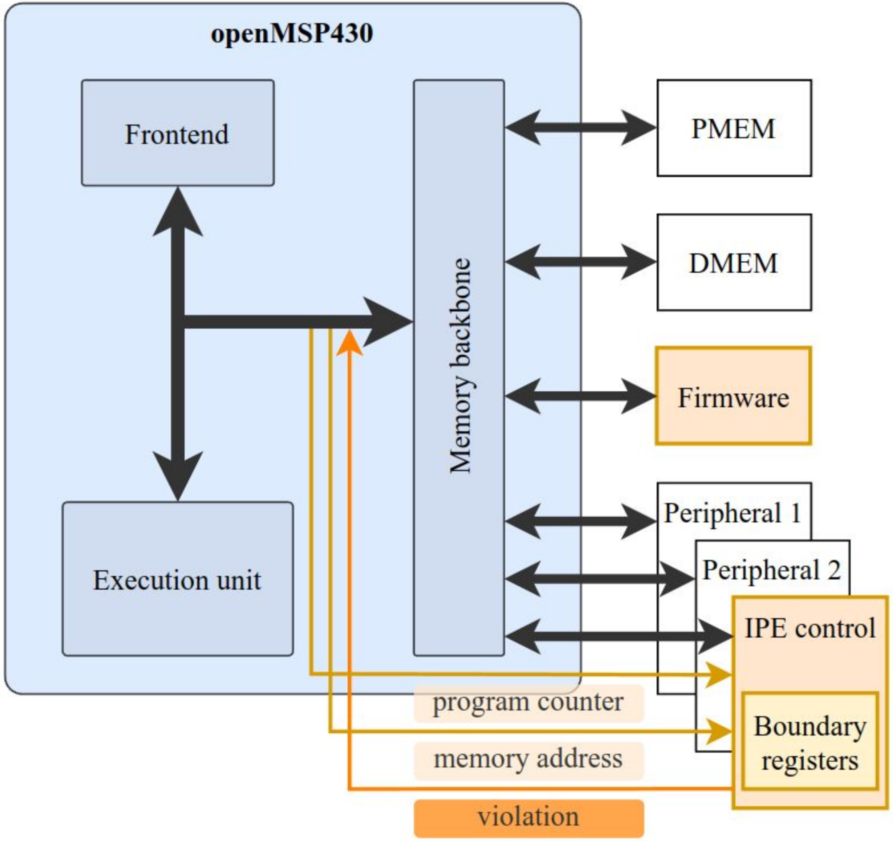
Our proposal: openIPE

- **Flexible isolation** primitive
  - Based on the IPE specification
  - With protected firmware
  - But freely configurable!

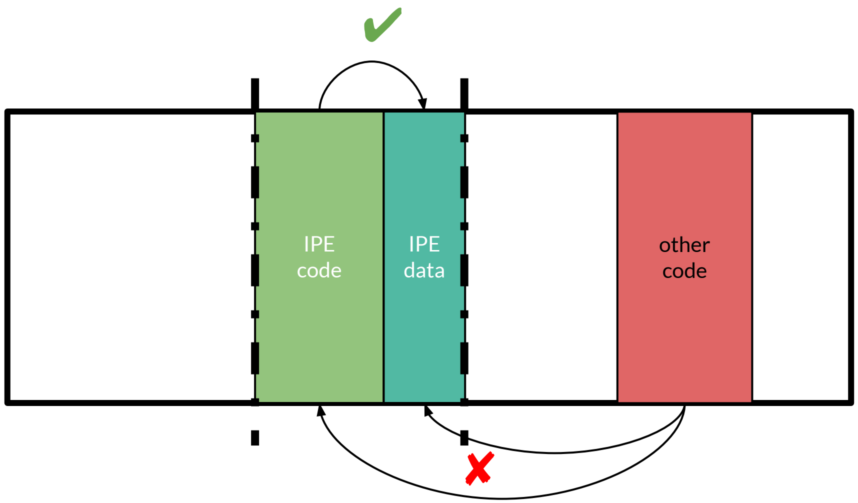


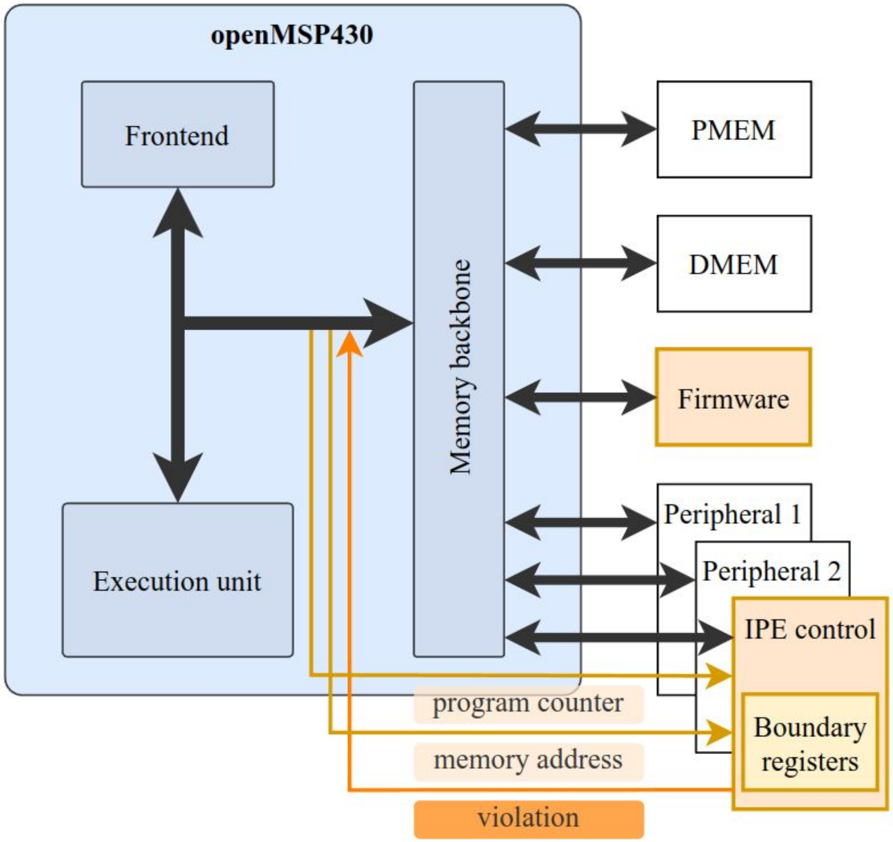
Our proposal: openIPE

- **Flexible isolation** primitive
  - Based on the IPE specification
  - With protected firmware
  - But freely configurable!
- Includes proposed **hardware fixes** for IPE



Our proposal: openIPE



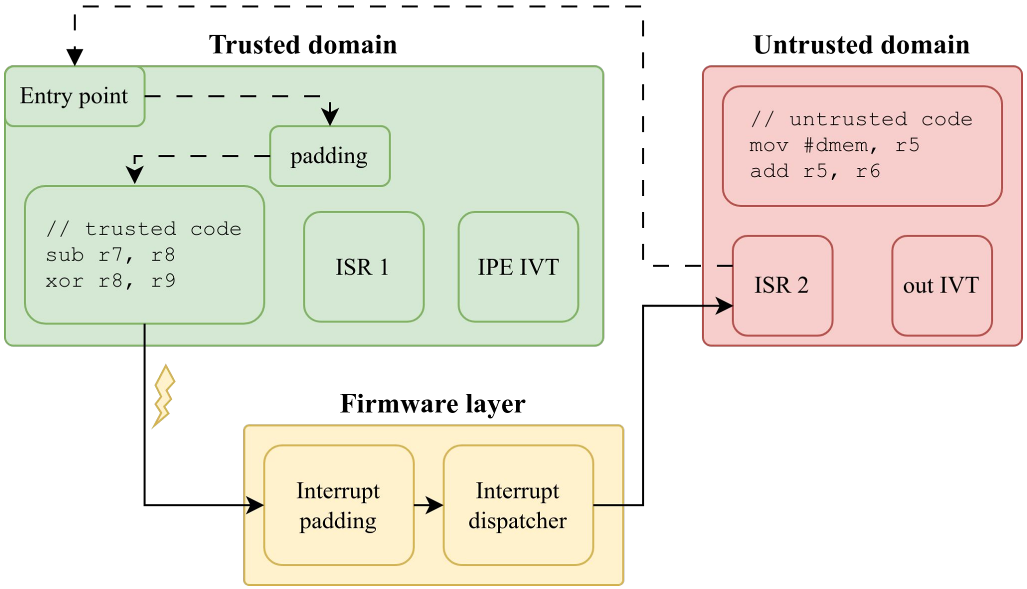


Case study: Secure interrupt handling

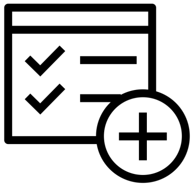
Approach	Secure scheduling	Architectural protection	Interrupt latency mitigation	Untrusted interrupts
Software disable	○	◐	●	○
Hardware disable	○	●	●	○
`SW-IRQ` (de Clercq, 2014)	◐	●	○	●
`FW-IRQ` *(our proposal)*	◐	●	●	●

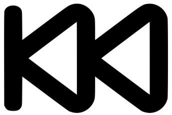
Case study: Secure interrupt handling

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



Hardware security validation: Unit tests





- Functional and security tests
- Backwards compatibility for (future) extensions

Hardware security validation: Unit tests

- Functional and security tests
- Backwards compatibility for (future) extensions

# 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

Software security validation: Symbolic execution

Issues reported at 0x81c4 2 ipe_func_internal CRITICAL Unconstrained read

Unconstrained read CRITICAL IP=0x81c4

Plugin extra info

Key	Value
Address	<BV16 r15_attacker_15_16>
Attacker tainted	True
Length	2
Pointer range	[0x0, 0xffff]
Pointer can wrap address space	True
Pointer can lie in enclave	True
Extra info	Read address may lie inside or outside enclave

Execution state info

Disassembly

```
000081b4 <ipe_func_internal>:
    81b4:       04 12           push    r4
    81b6:       04 41           mov     r1,     r4
    81b8:       24 53           incd    r4
    81ba:       21 83           decd    r1
    81bc:       84 4f fc ff     mov     r15,    -4(r4)  ;0xfffc(r4)
    81c0:       1f 44 fc ff     mov     -4(r4), r15     ;0xfffc(r4)
    81c4:       2f 4f           mov     @r15,   r15
    81c6:       21 53           incd    r1
    81c8:       34 41           pop     r4
    81ca:       30 41           ret
```

Alder et al. “Pandora: Principled Symbolic Validation of Intel SGX Enclave Runtimes”, S&P’24.

Summary

- **openIPE:** Open-source extensible memory isolation
  - Hardware + firmware + software co-design
- Framework for security validation
  - Unit test suite
  - Symbolic execution tool (Pandora)
- Fully open source!
  - https://github.com/martonbognar/openipe

openIPE

openIPE: An Extensible Memory Isolation Framework for Microcontrollers

CI passing License BSD 3-Clause