MPUsh: Applying Security Hotpatches Instead Of MPU Barriers

Christian Niesler, Christian Scholz, Lucas Davi
University of Duisburg-Essen

Proc. of 2nd Constructive Approaches for SeCurity Analysis and Design of Embedded systems Conference (CASCADE'26). Springer, Regensburg, Germany, 2026.

Hotpatching - First Aid for bleeding code

Rapid Response

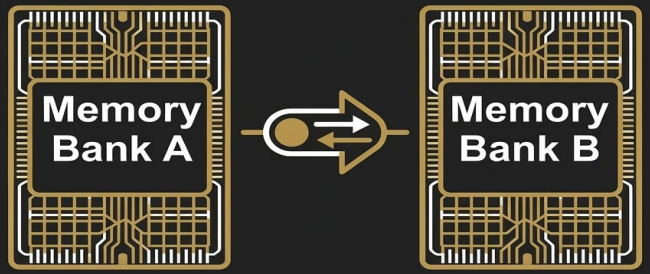
Rapid zero-day response without breaking timing guarantees

Continuous Availability

Continuous availability despite growing IoT attack surface

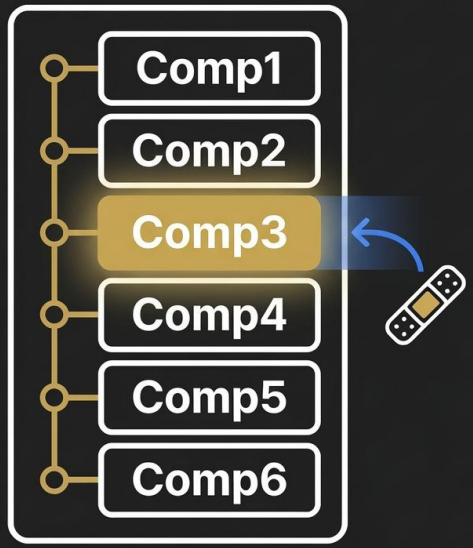
Hotpatching Origins

For hotpatching this requires:
full active-passive **system redundancy**



A/B PATCHING

Patching entire compartments,
is **replacing big blocks**



Compartmentalization Patching

Hotpatching Methods (State of the Art)

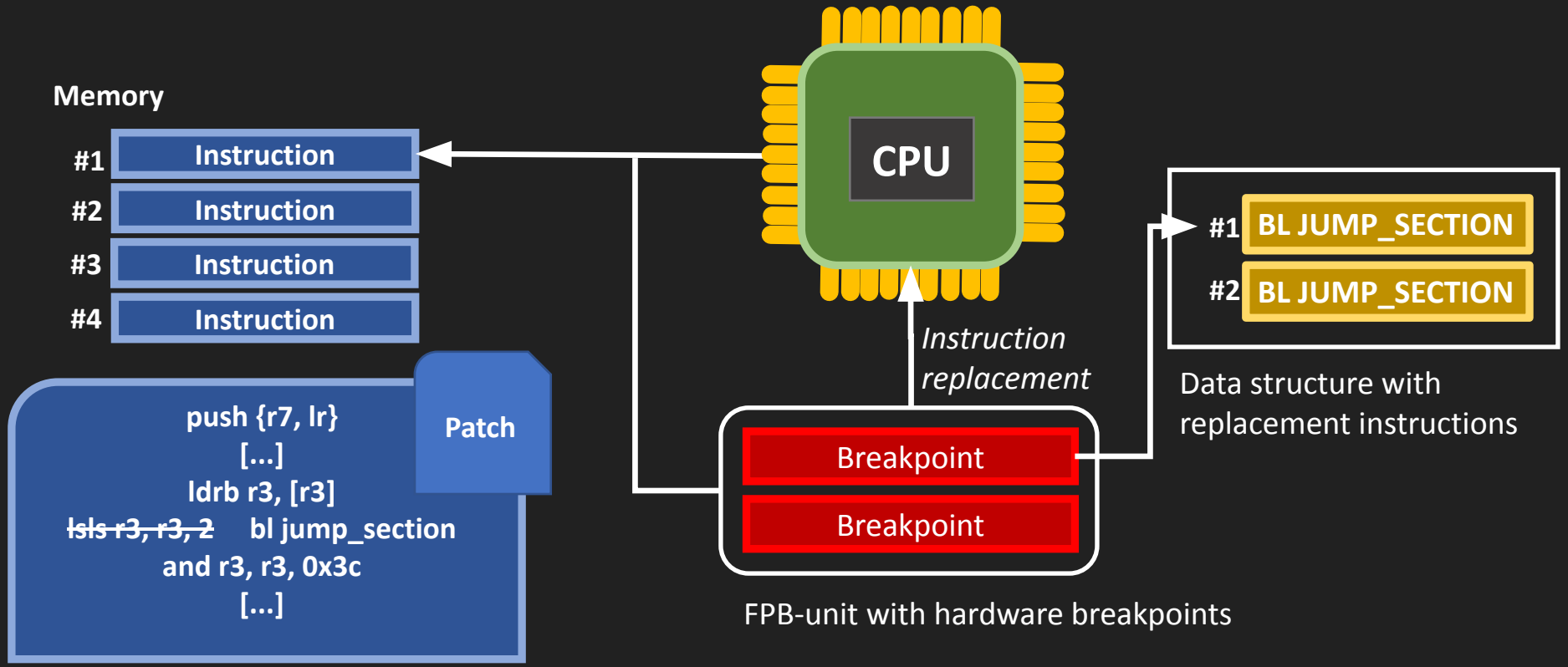
Hardware-Assisted Hotpatching Techniques

Dynamic Patching Through Pre-Compiled Patch Points

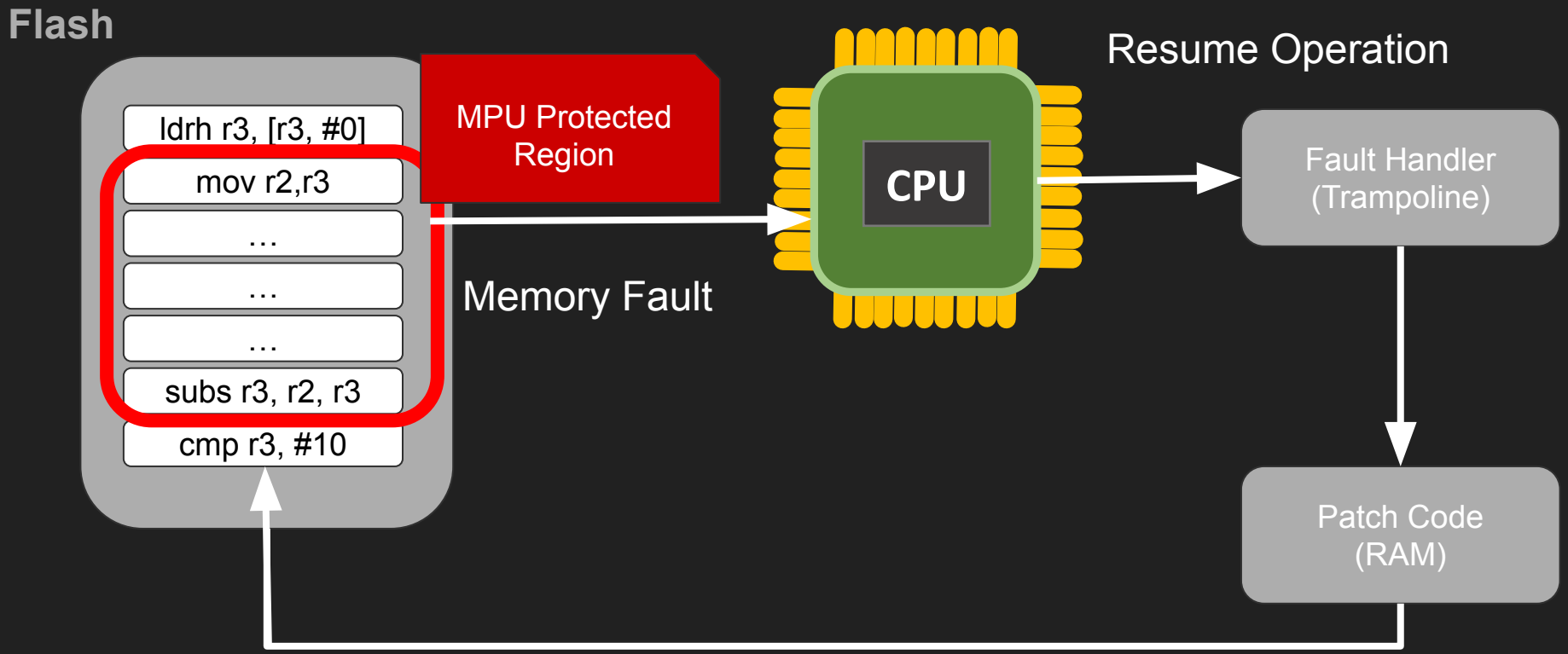
Code-Shadowing & Binary Rewriting

Related Work

HERA - **H**otpatching **E**mbedded **R**eal-Time **A**pplications



MPUsh


Flash
ldrh r3, [r3, #0]
mov r2,r3
…
…
…
subs r3, r2, r3
cmp r3, #10
MPU Protected Region
Memory Fault
CPU
Resume Operation
Fault Handler (Trampoline)
Patch Code (RAM)

Why MPUsh?

	MPUsh	HERA	RapidPatch	Kintsugi
PatchPoints	64 slots MPU regions	6-8 slots Breakpoints	theoretically unlimited pre-inserted hooks	unlimited code-shadowing binary rewriting
Redirection Speed				
Target Device	FLASH/RAM	FLASH/RAM	FLASH	RAM

Evaluation

Data in Clock Cycles

	MPUsh	HERA
Patch Activation	28	10
Patch Activation (Critical Step)	15	10
Flow Redirection	46 (136)	8,2

Limitations?

01 Manual patch generation

02 MPU Slot competition

03 Fault Handling Overhead

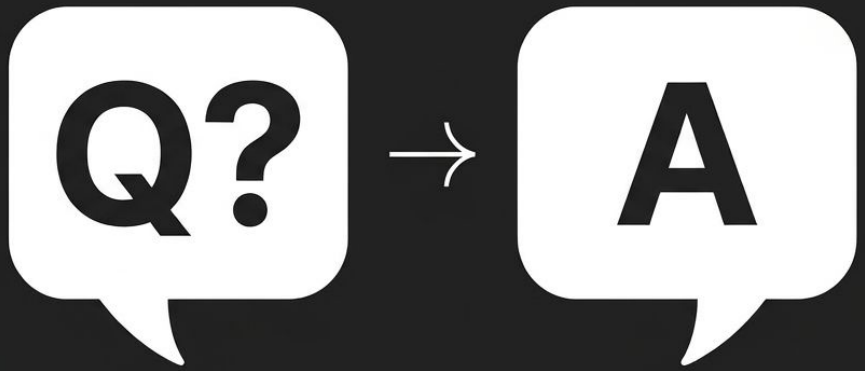
Contributions

01 MPU Hotpatch Trigger

02 15/46 clock cycle activation/redirection

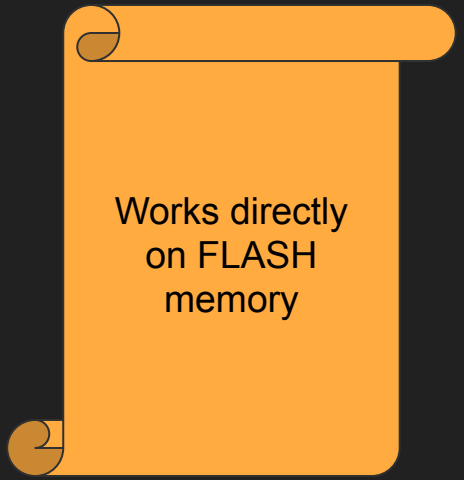
03 Syringe Pump proof-of-concept

Time for **Q**uestions and **A**nswers



Backup Slide Set

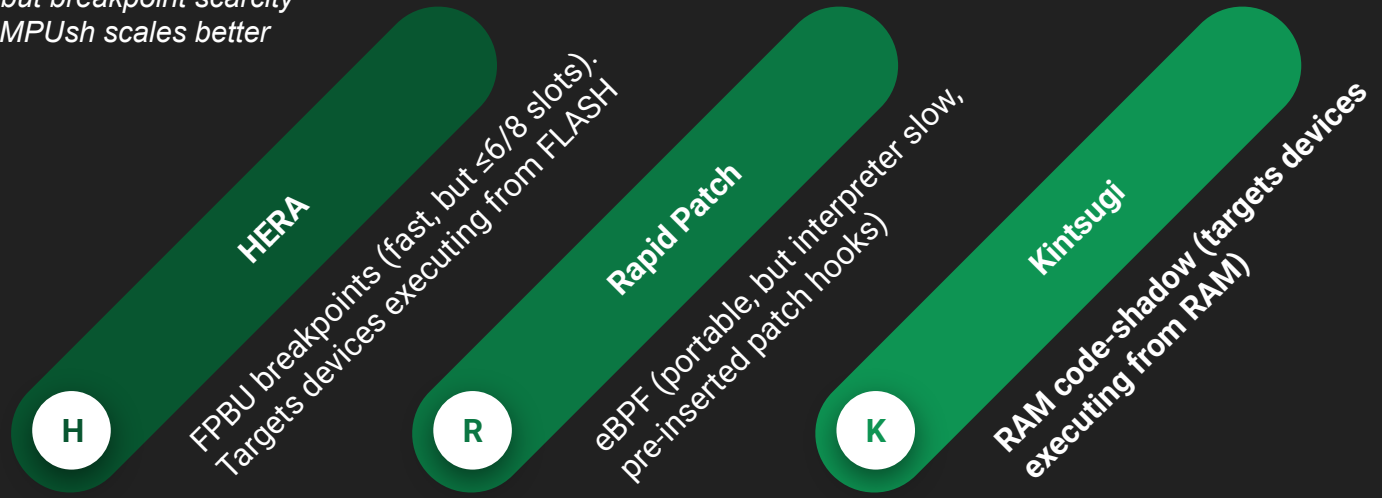
Why Hardware-Assisted Hotpatching?



Related Work

: ***Kintsugi*, scales and is reasonable quick, but targets code-shadow devices**

: ***HERA** is the fast, but breakpoint scarcity limits scalability → MPUsh scales better*



: ***RapidPatch** scales, but it very **slow,***
requires pre-inserted patch hooks

Why MPUsh?

	MPUsh	HERA
Patch Points	up to 64 patches (MPU regions and subregions)	up to 6-8 patches (available hardware breakpoints)
Portability	depends on MPU availability	depends on available debugging unit
Redirection Speed	~42 clock cycles	~8 clock cycles

Evaluation: case-study syringe pump
NUCLEO-F446RE (Cortex-M4)