24/02/2026

CHERI

CHERI Insights

Maja Malenko
CHERI Ambassador

The memory safety problem

⬡ Data breaches are very costly

- Cyberattacks cause more than $10 trillion of damage / year
  - ❑ Emergency response, system repair, security updates and patching, legal fines, customer compensation, and even lost business

~$10T

Worldwide cost estimate of cyberattacks per year

(and growing fast)

>$500M

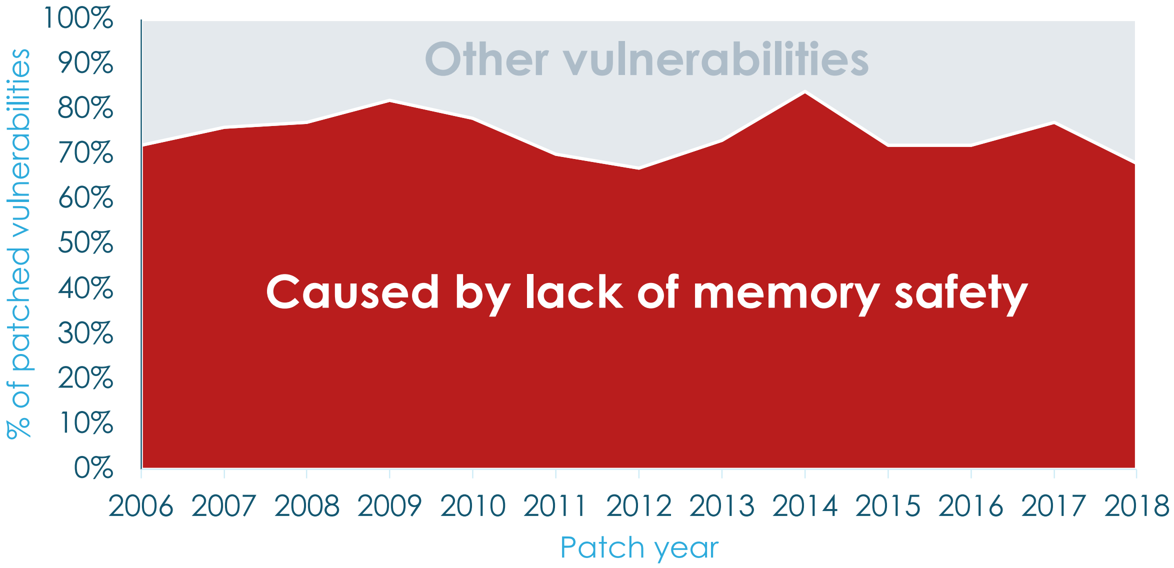
Cost of addressing Heartbleed buffer overflow vulnerability

6X

Increase in firmware attacks reported by NIST between 2017 and 2024

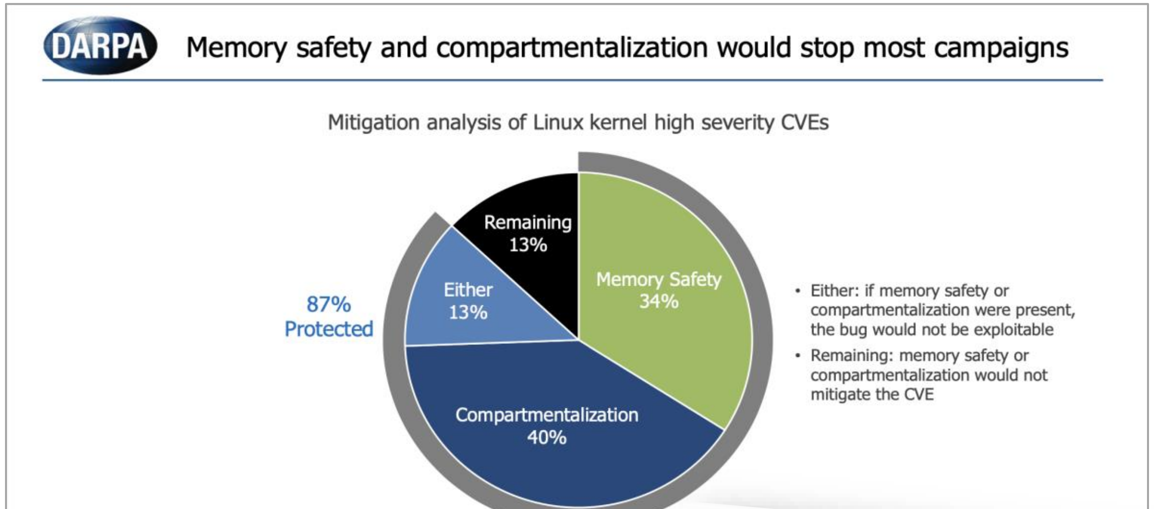
Solving the worst cybersecurity issue

- Most attacks due to a lack of **memory safety**
  - **Microsoft says 70%** of software vulnerabilities are due to unsafe memory accesses in C/C++
  - **MITRE's CWE Top 25** list (based on ~39,000 CVEs) shows memory safety issues
- Unsolvable problem with traditional software solutions (new languages, practices, tools)
- **CHERI** solves the memory safety problem



Source: Trends, challenge, and shifts in software vulnerability mitigation - Microsoft 2019

Memory safety becomes a key topic



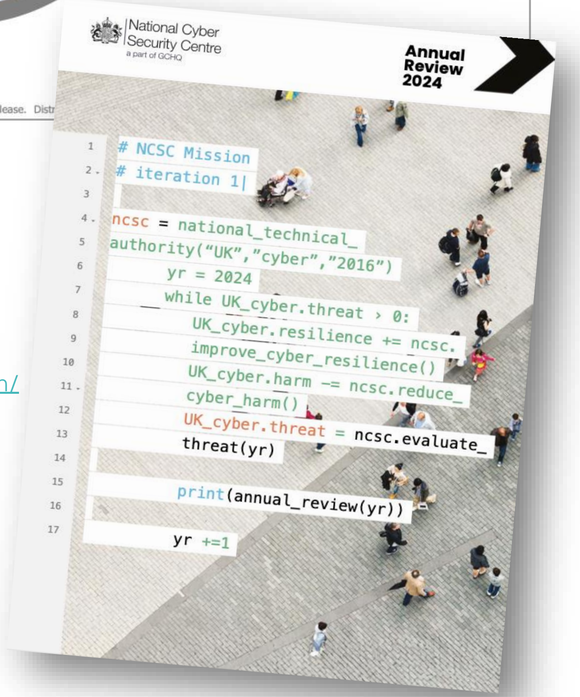
DARPA Memory safety and compartmentalization would stop most campaigns

Mitigation analysis of Linux kernel high severity CVEs

- Either: if memory safety or compartmentalization were present, the bug would not be exploitable
- Remaining: memory safety or compartmentalization would not mitigate the CVE

CVE: Common Vulnerabilities and Exposures

Distribution Statement A: Approved for public release. Distr



National Cyber Security Centre a part of GCHQ

Annual Review 2024

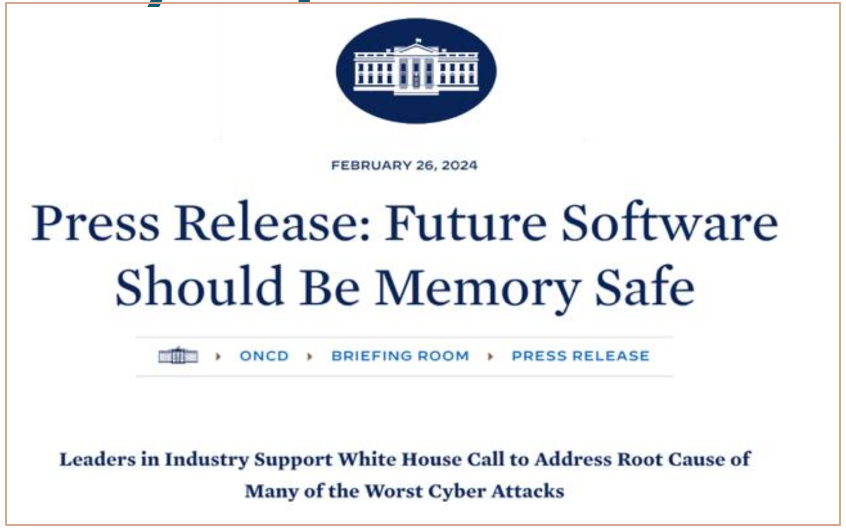
```
# NCSC Mission
# iteration 1|

ncsc = national_technical_
authority("UK","cyber","2016")
    yr = 2024
    while UK_cyber.threat › 0:
        UK_cyber.resilience += ncsc.
        improve_cyber_resilience()
        UK_cyber.harm -= ncsc.reduce_
        cyber_harm()
        UK_cyber.threat = ncsc.evaluate_
        threat(yr)

    print(annual_review(yr))

    yr +=1
```

https://www.ncsc.gov.uk/collection/ncsc-annual-review-2024



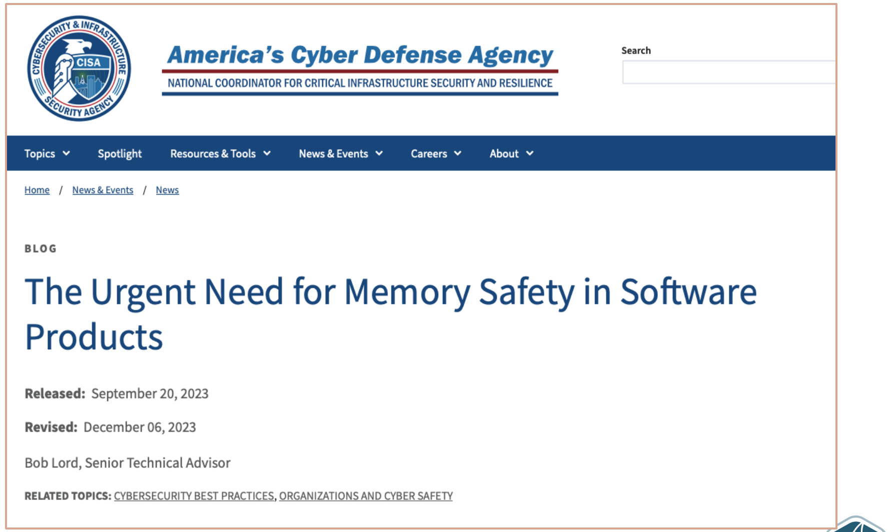
FEBRUARY 26, 2024

Press Release: Future Software Should Be Memory Safe

Leaders in Industry Support White House Call to Address Root Cause of Many of the Worst Cyber Attacks

Highlight CHERI as a solution

Article: https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/02/26/press-release-technical-report/
Report: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf
(CHERI mentioned on p9)



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

BLOG

The Urgent Need for Memory Safety in Software Products

Released: September 20, 2023

Revised: December 06, 2023

Bob Lord, Senior Technical Advisor

RELATED TOPICS: CYBERSECURITY BEST PRACTICES, ORGANIZATIONS AND CYBER SAFETY

https://www.cisa.gov/news-events/news/urgent-need-memory-safety-software-products

> As noted by the White House in a recent report on a path toward secure and measurable software, hardware support is critical to robust and efficient memory safety. Compiling software to run on CHERI enhanced processors guarantees very strong memory safety that an attacker cannot bypass

Professor Simon Moore,
University of Cambridge

Europe's Cyber Resilience Act (CRA)

- EU is making cybersecurity a legal requirement, not just a best practice.
- The CRA requires software and IoT products in the EU to be **secure by design**.
  - Full enforcement is due by December 2027
- It holds manufacturers legally responsible for security and updates throughout a product's lifetime
  - **CHERI** helps companies meet the CRA by preventing memory vulnerabilities in hardware

Possible solutions for memory safety

✗ Use memory safe languages like Rust

- Requires rewriting **trillions** of lines of C/C++ code, compared to ~**40M** in Rust
- Possible (and good) for new code, but no compartmentalisation
- Rust still has unsafe code (runtime and libraries)

✗ Use coarse-grained techniques like stack canaries to detect issues

- Helpful, but they **statistically** leave too many holes
- Can still be bypassed

✓ Use fine-grained techniques like CHERI

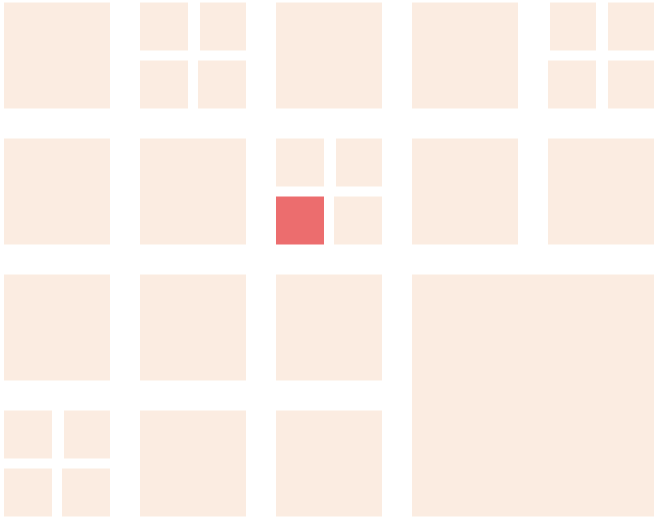
- Best option, but needs new hardware

What is CHERI?

C	apability
H	ardware
E	nhanced
R	ISC
I	nstructions

Hardware-based solution to a software problem

- CHERI is an open modern **capability** architecture
  - ✓ A **hardware-based approach** to memory safety
  - ✓ Brings strong security to **existing code**
  - ✓ 15 years of development by University of Cambridge (UK) / SRI (USA)
  - ✓ Formally proven ISA
- Strong, fine-grained **memory protection**
  - ✓ Hardware enforced
  - ✓ **Deterministic**
- **Scalable compartmentalization**
  - ✓ Principle of least privilege



Compartmentalization prevents contagion

CHERI backed by strong supporters

National Cyber Security Centre
a part of GCHQ

DARPA

UKRI UK Research and Innovation

Microsoft

Google

UNIVERSITY OF CAMBRIDGE

arm

BT

Codasip

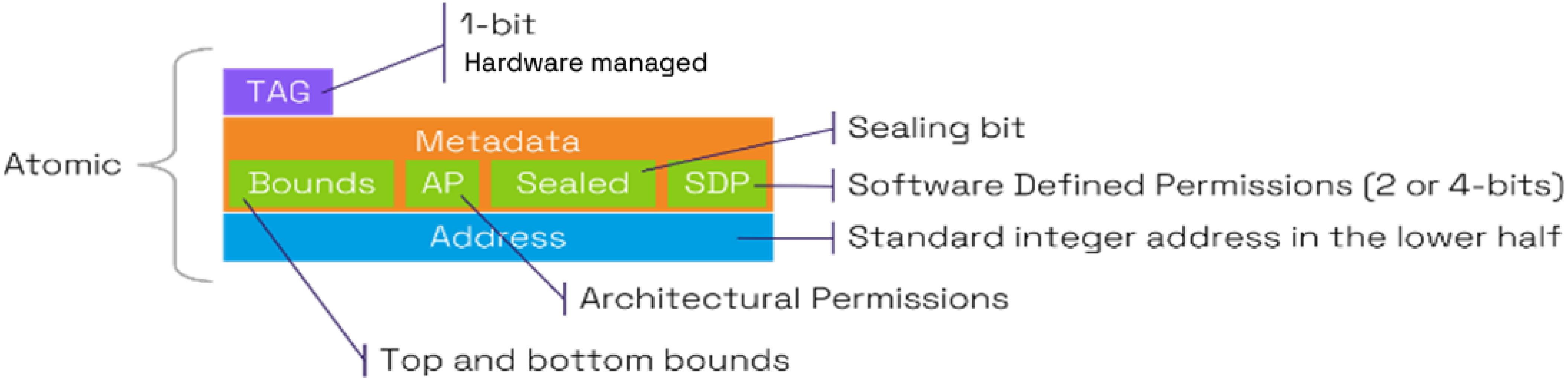
SRI

✚ many other members of the CHERI Alliance
https://cheri-alliance.org/member/

~ $300 million investment in the development of CHERI
(by governments and industry)

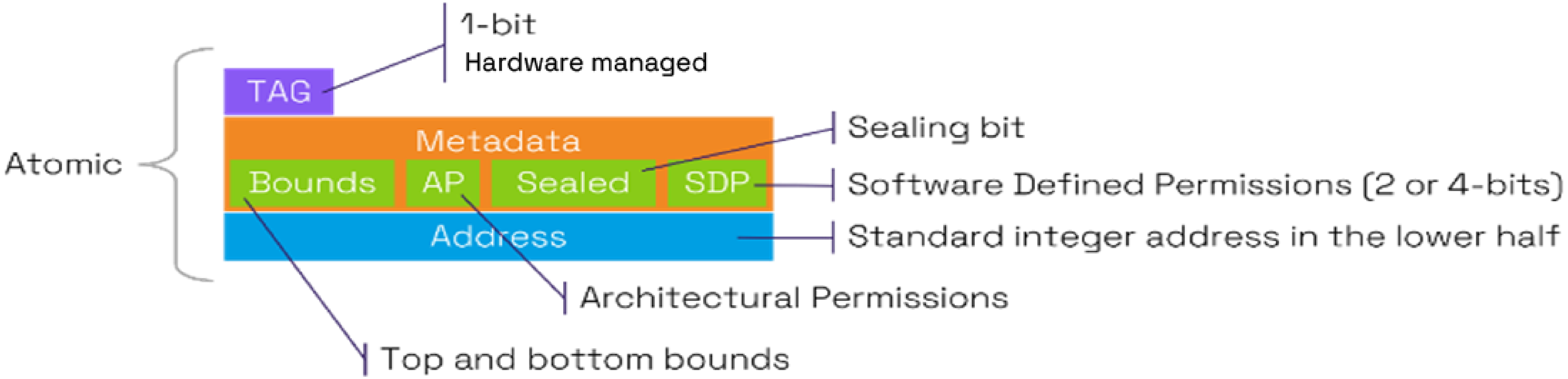
⬡ CHERI Capabilities

- Capabilities are new architectural primitives
  - **Metadata** (bounds, permissions, …) control how they are used
  - **Tags** protect integrity
  - **Guarded manipulation** controls how they are manipulated (e.g., provenance validity and monotonicity)


1-bit
Hardware managed
TAG
Atomic
Metadata
Bounds
AP
Sealed
SDP
Address
Sealing bit
Software Defined Permissions (2 or 4-bits)
Standard integer address in the lower half
Architectural Permissions
Top and bottom bounds

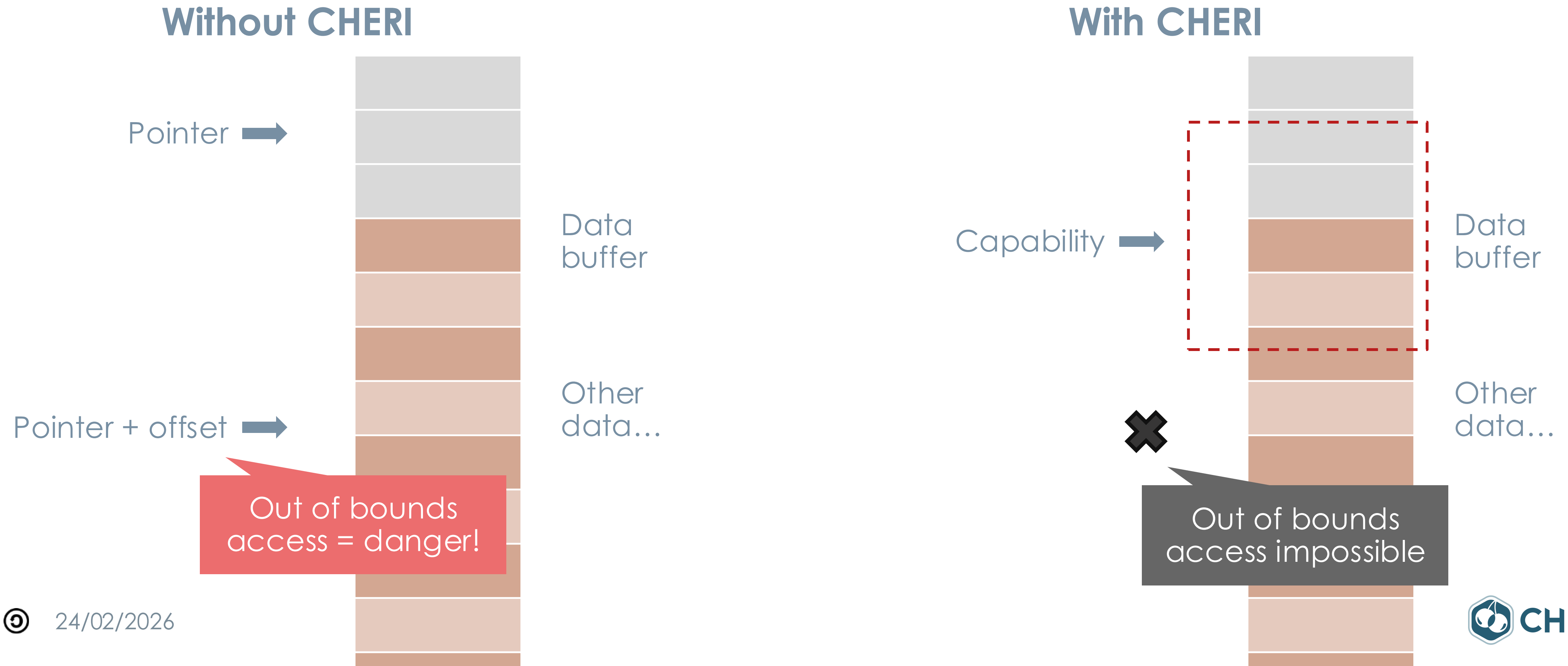
CHERI Capabilities

- Properties
  - ✓ **Integrity** and **provenance validity** ensure capabilities cannot be forged
  - ✓ **Bounds** prevent accessing the wrong object
  - ✓ **Monotonicity** prevents privilege escalation (bounds and permissions cannot be increased)


1-bit
Hardware managed
TAG
Atomic
Metadata
Bounds
AP
Sealed
SDP
Address
Sealing bit
Software Defined Permissions (2 or 4-bits)
Standard integer address in the lower half
Architectural Permissions
Top and bottom bounds

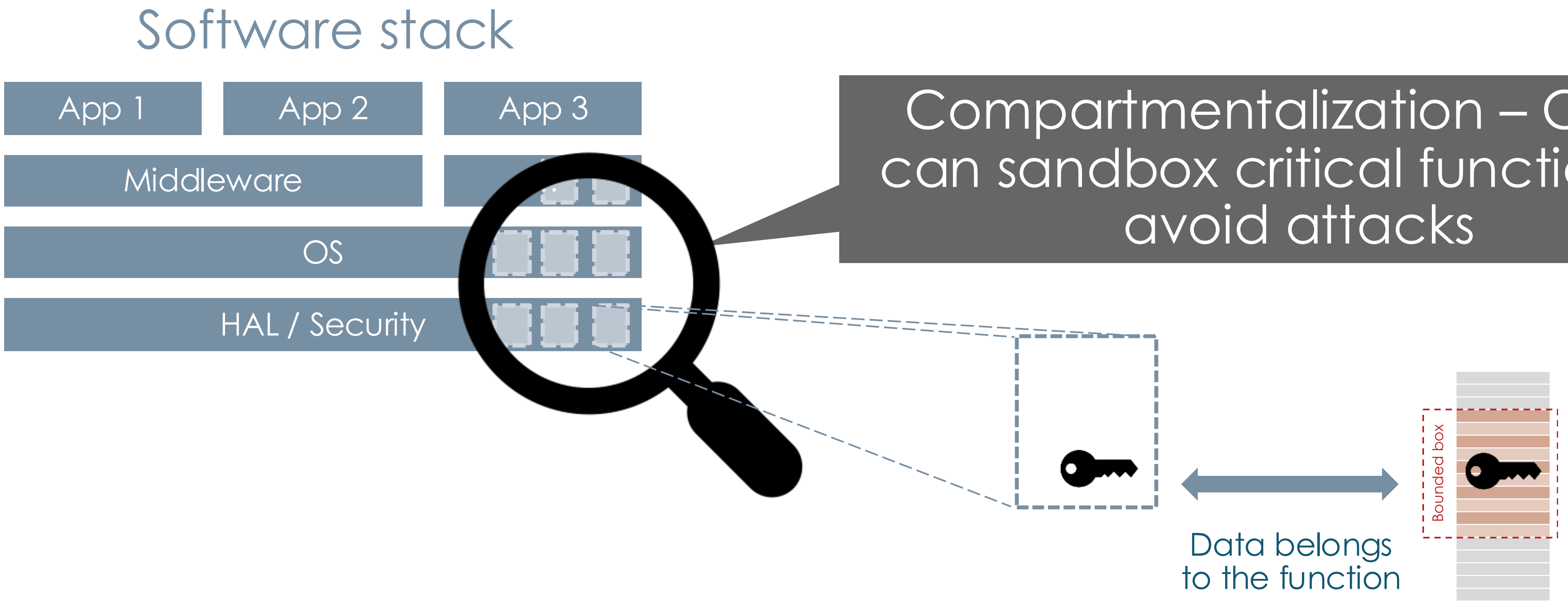
CHERI brings memory safety

- Replacing pointers by capabilities – with hardware control



CHERI brings compartmentalization

- Capabilities belong to an identified function / execution context

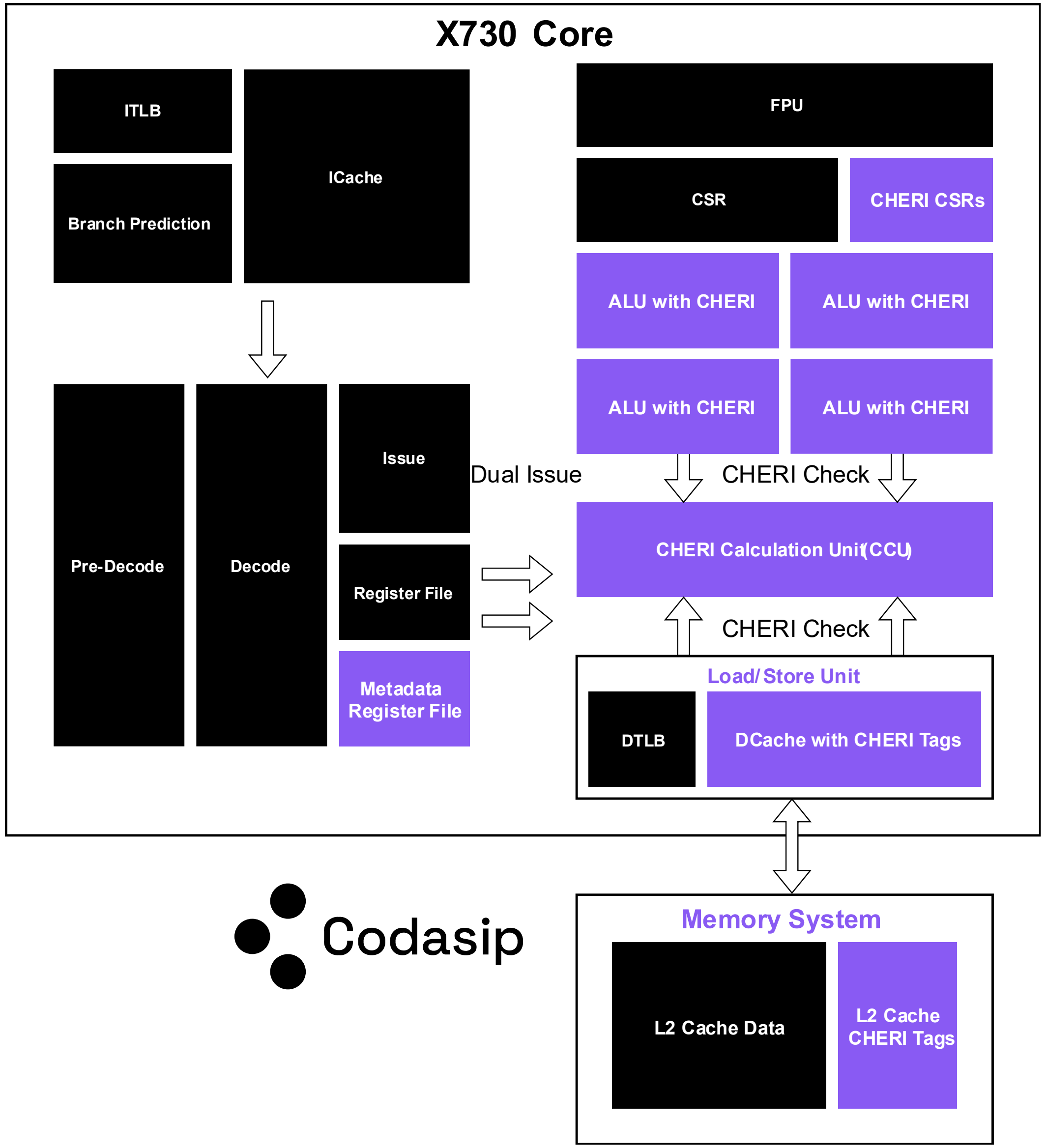


Compartmentalization – CHERI can sandbox critical functions to avoid attacks

CHERI hardware changes

- New instructions
  - ✓ Manipulating capabilities
  - ✓ Dereferencing capabilities
- Capability-extended registers
- Tagged memory

- **ISAs**
  - ✓ Arm, RISC-V
    - but also x86, MIPS



Codasip

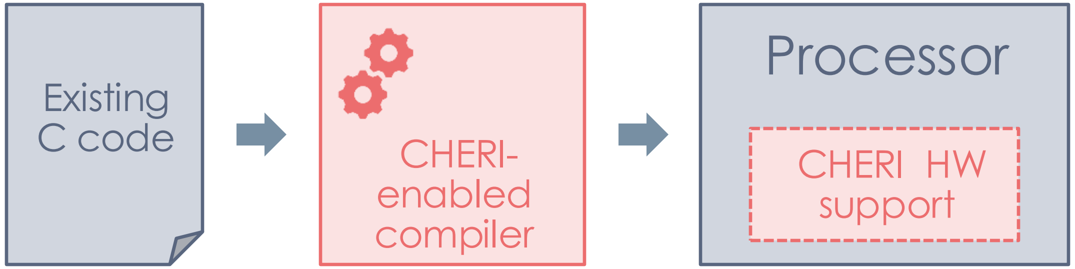
CHERI

CHERI adoption

(costs, benefits)

CHERI relies on hardware protection

- CHERI requires adapted processor
- Reuse existing code
  - ✓ Little modifications to an application mostly recompile & optimize
  - ✓ Create CHERI compartments for critical code secrets remain secret
- Low impact but **huge gains**
  - ✓ Area & Power < 5% more at CPU level
  - ✓ Performance ~3-5% less (work in progress – still improving)
  - ✓ Performance gains with compartmentalization
  - ✓ Memory impact
    - Tag storage and capabilities



CHERI hardware projects and products

- Arm Morello board arm Morello Program
  - ✓ High-end 64-bit research application processor
- Codasip X730 Codasip
  - ✓ Mid-range 64-bit application processor
- CHERIoT Sonata board lowRISC
  - ✓ Low-end 32-bit microcontroller
- CHERI RISC-V standard ratified soon
  - ✓ https://github.com/riscv/riscv-cheri

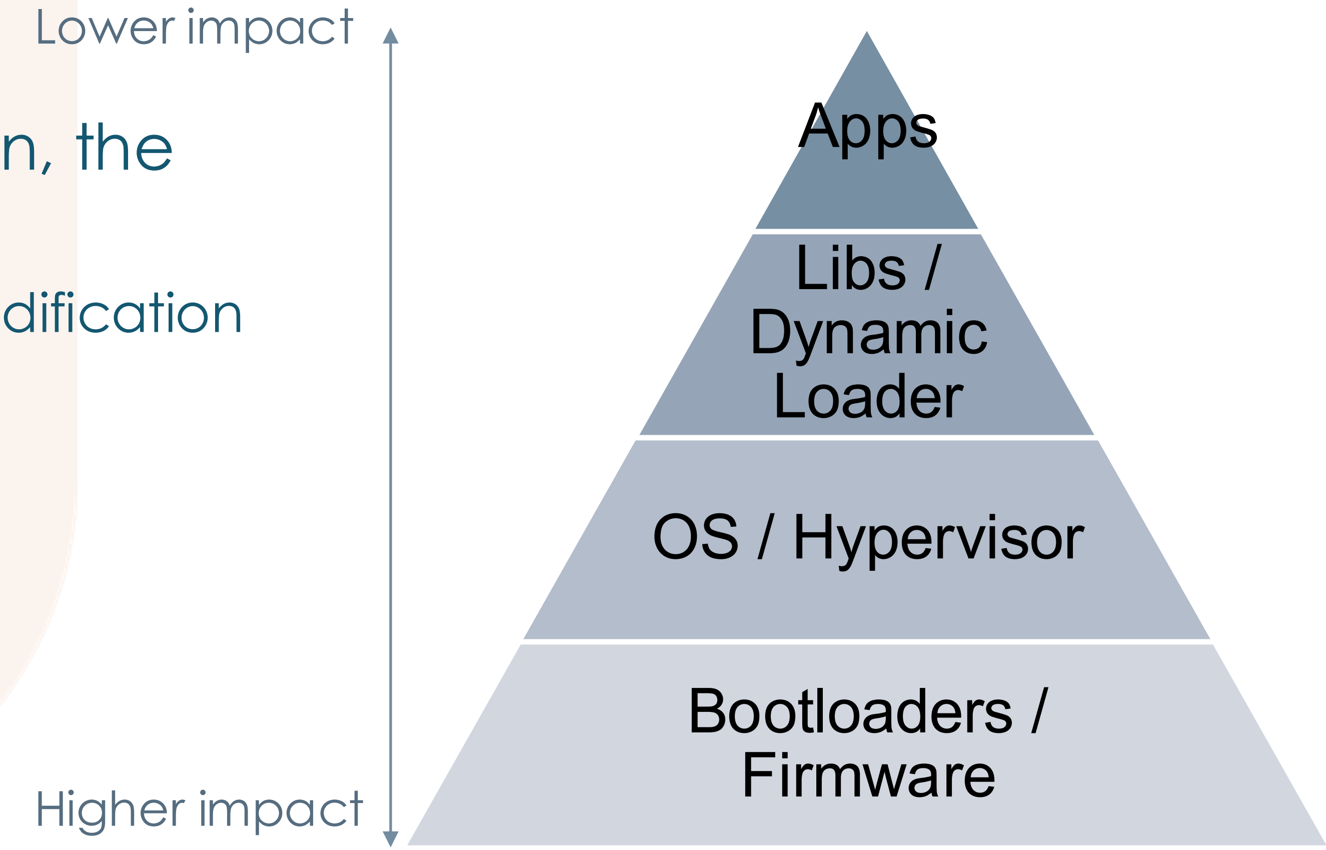
Now collaborating as part of the

CHERI Alliance

- Support HW/SW ecosystem
- Solve common problems
- Joint promotion

CHERI software impact

- Any code that manages memory safety need to be adopted to CHERI
- The higher the level of abstraction, the less code change required
  - ✓ Applications often need minimal modification (~ 0.1%)
  - ✓ Nginx (0.1% - 0.5%)
  - ✓ FreeBSD (1% - 2%)
- OSs ported to CHERI
  - ✓ CHERIBSD, Linux, seL4, VxWorks, ...
  - ✓ CHERIoT RTOS, FreeRTOS, Zephyr, ThreadX, …



Organized by the CHERI Alliance

CHERITech

- Technical focus
  - Free entry (even non-members)
  - Talks, demos, workshops
  - Research updates
- Next edition
  - CHERITech’2025
  - 14th November 2025
  - Manchester

CHERI Blossoms Conference

- Main event
  - Free entry (even non-members)
  - Talks, demos, networking
  - Published online
- Next edition
  - CHERI Blossoms Conf 2026
  - 26-27th March 2026
  - Cambridge

embeddedworld
Exhibition&Conference

See all events: https://cheri-alliance.org/events/

CHERI

CHERI Alliance Members

axiomise® predictable formal verification

BT

cantech informatics

CAPABILITIES LIMITED

CHEVIN TECHNOLOGY

Codasip

Critical technologies inc. Trustworthy Networked Autonomy

CyberWhiz

CYNAM

CATAPULT Digital

discribe IMAGINING SECURE DIGITAL FUTURES

[dstl]

FreeBSD FOUNDATION

Google

LMT

lowRISC

MISRA

National Cyber Security Centre a part of GCHQ

nquiringminds

PARVAT

SIEMENS

SCI Semiconductor

SRI

TRUSTED COMPUTING CENTER OF EXCELLENCE

TechWorks

VeriSilicon

ZAYA

WYVERN GLOBAL

جامعة الملك عبدالله للعلوم والتقنية King Abdullah University of Science and Technology

RPTU

UNIVERSITY OF BIRMINGHAM

UNIVERSITY OF CAMBRIDGE

University of Kent

University of Glasgow

MANCHESTER 1824 The University of Manchester

Prifysgol Abertawe Swansea University

Updated list and members’ details
https://cheri-alliance.org/memberships/

CHERI

Benefits of CHERI

Strongest memory protection	Hardware-based Security by design
Reuse existing software	Recompile Fix Optimize
Open technology	No IP protection
Very **low impact**	~ 4% additional processor cost Same product development costs Same or better * performance

* Higher performance after code optimization for CHERI

CHERI

THANK YOU

Contact: maja.malenko@cheri-alliance.com

Web: www.cheri-alliance.org