14 March 2025

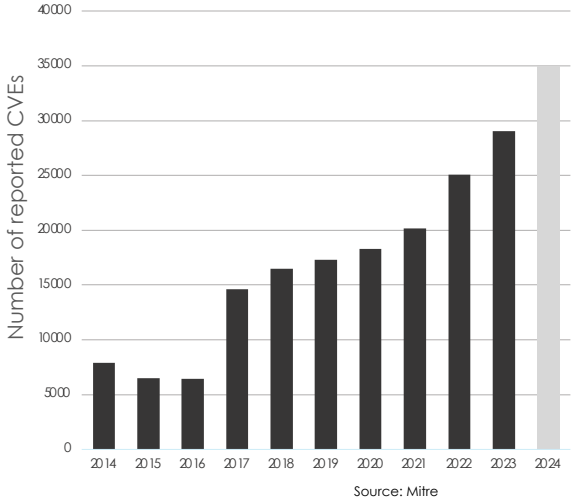

# CHERI technology overview

## A quick introduction

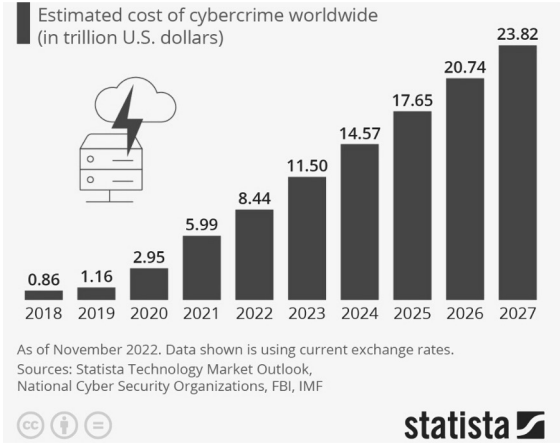
# Data breaches are very costly

| >$500M | 6X | ~$10T |
| --- | --- | --- |
| Cost of addressing Heartbleed buffer overflow vulnerability | Increase in firmware attacks reported by NIST between 2017 and 2024 | Worldwide cost estimate of cyberattacks per year (and growing fast) |

# Software vulnerabilities are causing increasing risk

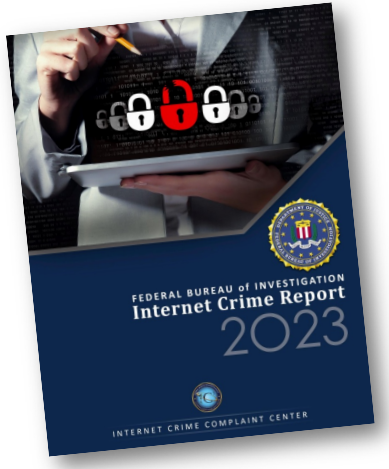



Source: Mitre



# Cyberattacks a significant problem

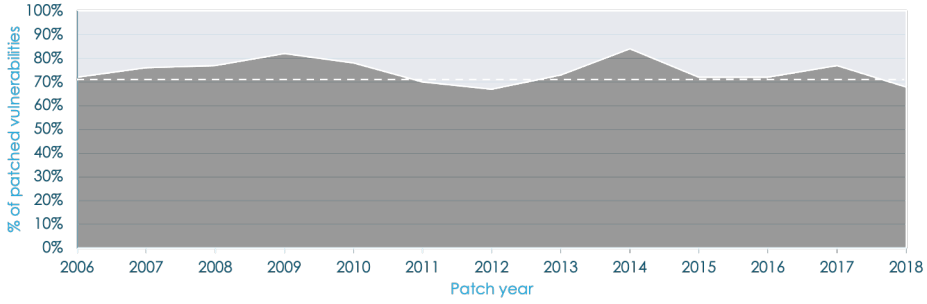
- Example in the USA…
  - $12.5 billion loss in 2023
    - **20% increase** vs 2022
  - Major under-reporting…
    - Report only contains what is declared to the FBI




https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

# Memory safety is necessary

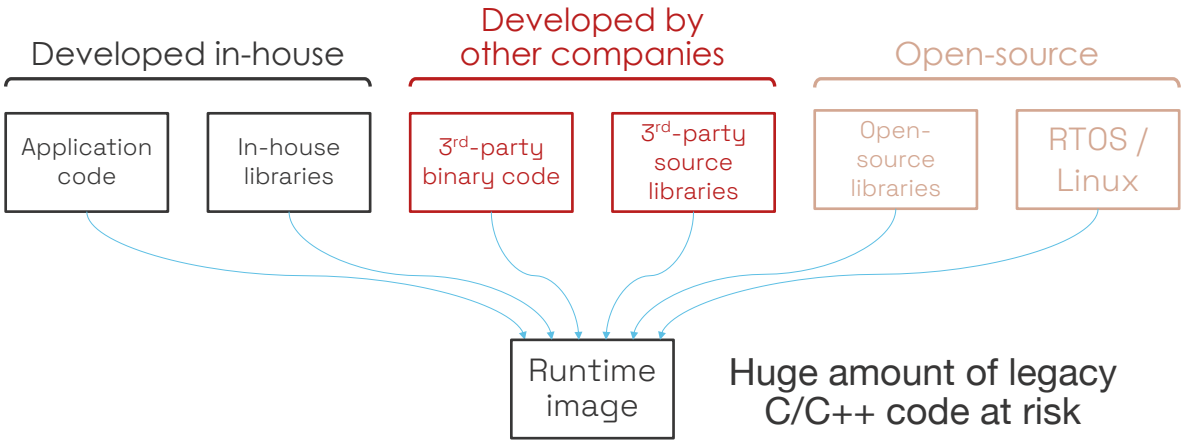
- Memory abuse (e.g. buffer overflows) is the main attack vector
- Constant ratio of over the past 20 years
  - … even with all the work done on software to avoid this!




CHERI solves this!

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

# Impossible to re-write software to fix the problem



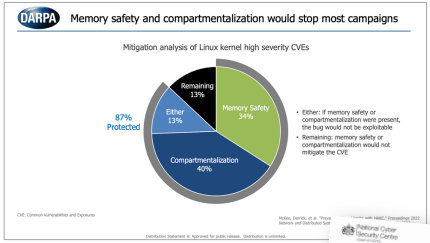
# Possible solutions for memory safety

✗ Use “memory safe” languages like Rust or .Net
- Requires rewriting trillions of lines of C/C++ code
- Possible for new code, but no compartmentalisation

✗ Use “coarse-grained” techniques like stack “canaries” to detect issues
- Helpful, but they statistically leave too many holes
- Hacking techniques already developed

✓ Use “fine-grained” techniques like CHERI
- Best option, but needs new hardware

# Memory safety becomes a key topic





FEBRUARY 26, 2024

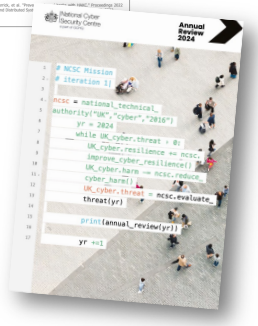
Press Release: Future Software Should Be Memory Safe

ONCD › BRIEFING ROOM › PRESS RELEASE

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)




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


America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Topics Spotlight Resources & Tools News & Events Careers About

Home / News & Events / News

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

# CHERI technology

**C** apability
**H** ardware
**E** nhanced
**R** ISC
**I** nstructions

# About CHERI

- Initiated by a project from


- Originally developed by



- Matured for 14 years
- Supported by

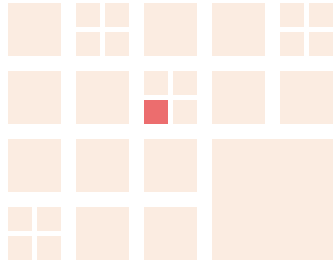


**~ $300 million investment in the development of CHERI**

(by governments and industry)

# CHERI

- A new **hardware-based approach** to memory safety
- Strong, fine-grained **memory protection**
  - Hardware enforced
  - Deterministic
- **Compartmentalization**
  - Principle of least privilege



Compartmentalization prevents contagion

# What makes CHERI different?

| | Previous solutions | Problem | CHERI |
|---|---|---|---|
| **Security control** | Statistical<br>• "likely" to detect a problem | Targeted attacks bypass protection<br>Some problems detected too late | Systematic<br>• 100% coverage |
| **Enforcement** | Some complex, disparate hardware features, no coherency across architectures<br>Rely on "trusted" software and/or explicit checks | Additional complexity<br>Software can be hacked (and has been…) | Hardware-enforced<br>• Simple, holistic protection<br>• No way to bypass by software (unforgeable tags) |
| **Software impact** | High impact on software<br>• A lot of additional code needed to protect and isolate<br>• Need best security experts to review all software stack<br>• Often need to rewrite code | Difficult to catch all issues<br>Reduce performance and increase code size<br>Experts are scarce | Extremely low software impact<br>• Need recompilation<br>• Adapt some very low-level code |
| **Type of solution** | Reactive<br>• Fix problem if vulnerability discovered<br>Proactive solution possible (but uneconomical) | Huge exploitable attack surface, susceptible to 0-day attacks<br>Most systems are not upgraded immediately / regularly | Preventive<br>• Protects against existing and to-be-designed attacks on memory |

# Main memory issues with C/C++

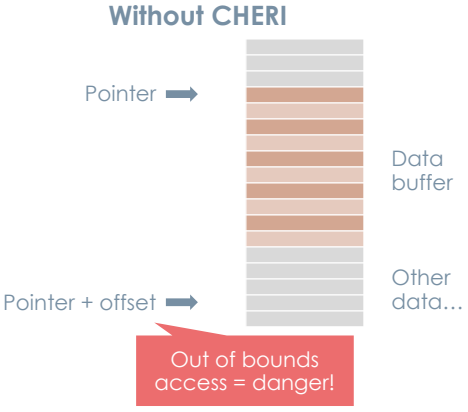
- Possible to access memory out of expected buffers
  - Access confidential data
  - Modify / delete critical data or code
  - Inject malware code
  - Spy on communications
  - Erase traces of attack
- Functions cannot protect their data from each other
  - Only works when the software can be trusted
  - Enable privilege escalation

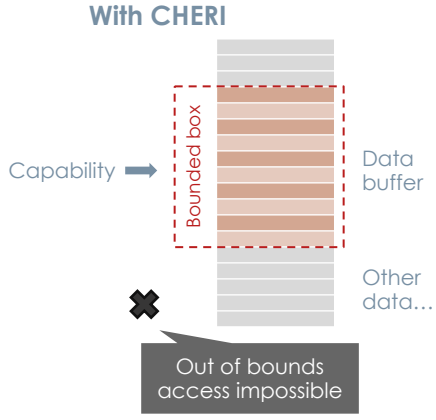
Need memory safety

Need compartmentalization

# Spatial memory safety

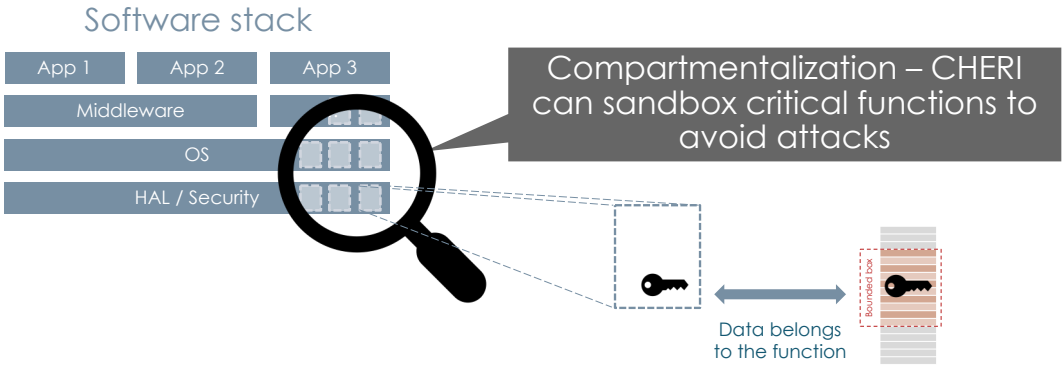
- Replacing pointers by capabilities – with hardware control



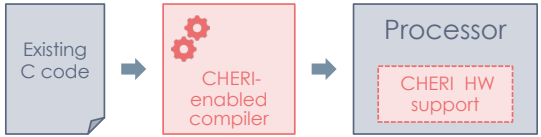
# Compartmentalization

- Capabilities belong to an identified function / execution context



# CHERI relies on hardware protection

- CHERI requires adapted processor
  - Can be applied to many types of core
- Hardware-enforced security
  - Impossible to bypass by software
  - Formally proven
- Reuse existing code
  - Just recompile application
  - Choose which part to protect
- Benefit from CHERI
  - Rejects dangerous code
  - Create CHERI compartments for critical code



# CHERI has a positive impact

## Limited costs

- Area impact
  - Processor only 4% larger*
  - Similar power consumption
  - Similar performance**
- Memory impact
  - Small area for tag storage
  - Double size for pointers (mostly impacts stack)
  - No change on data storage requirements
- Software development
  - Need adapted tools (open-source available)
  - Less than 0.5% application code*** to adapt
  - Need recompilation
  - OS / low-level drivers need work (done once)

## Huge gains

- Memory safety!
  - Save in patching costs
  - Compiler detects mistakes in existing code
- Performance gains****
  - Remove or simplify software-based mechanisms (TEE, compartmentalization, security modes, …)
  - Eliminate context switching in hypervisor
  - Reduce code, improve execution speed
- Fast, low-risk integration of unsafe code
- Save security experts' time
  - Not wasting it on bug hunting…

CHERI Alliance will help by stimulating the ecosystem to adapt OS / software / tools

* Real data from Codasip – Comparing the same commercial processor with/without CHERI
** Slight degradation for chips with low-bandwidth internal bus (i.e. less than 128bit)
*** Real data from application porting
**** Requires OS / security mechanisms adaptation (done once, usually by the ecosystem)

# Benefits of CHERI for functional safety

- Reduce development and certification costs
  - Simplifies the analysis of source code
  - Demonstrate absence of memory vulnerabilities
- Allow modern development
  - No need for strict MISRA-C or SAFE-C constraints
  - Use all features of the C language
  - Enable innovation and new features
- Enable consolidation of multiple functions on a chip
  - Watertight isolation
  - Reduces cost and complexity

# CHERI has already got strong supporters










# CHERI projects / products

- Prototypes / proof of concept
  - Proof of concept

    
    arm Morello Program
  - Open-source / prototype

    
    
- Commercial use

  
  
- OS ported to CHERI (Free RTOS, Zephyr, Linux, FreeBSD, seL4…)

The CHERI architecture's support for fine-grain memory protection and scalable compartmentalization promises to revolutionise our ability to protect personal data and provide strong defences against malware on mobile devices and in the cloud

*Ben Laurie, Director of Security,*
***Google Research***

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***

CHERI

# THANK YOU

Contact contact@cheri-alliance.org

Web www.cheri-alliance.org