



UK Research
and Innovation

Digital Security by Design - DSbD

MPSoC 2025

John Goodacre

Prof. Computer Architectures
University of Manchester

Director, Security and Resilience
UK Research and Innovation
Innovate UK

Why after 50+ years is cybersecurity still based on **patching** and **retrofitting** security?

The panel cannot overemphasize its belief that "patching" of known faults in the design or implementation of existing systems without any better technical foundation than is presently available, is futile for achieving multilevel security.

Unless security is designed into a system from its inception, there is little chance that it can be made secure by retrofit.

ESD-TR-73-51, Vol. I

COMPUTER SECURITY TECHNOLOGY PLANNING STUDY

James P. Anderson

October 1972

DEPUTY FOR COMMAND AND MANAGEMENT SYSTEMS
HQ ELECTRONIC SYSTEMS DIVISION (AFSC)
L. G. Hanscom Field, Bedford, Massachusetts 01730

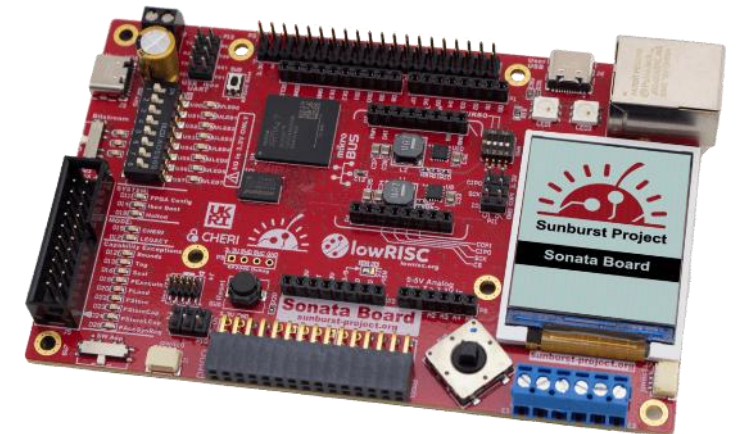
Approved for public release;
distribution unlimited.

(Prepared under Contract No. F19628-72-C-0198 by James P. Anderson & Co.,
Box 42, Fort Washington, Pa. 19034.)



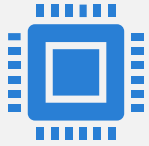
MPSoC 2022: Spoke about a UK response..

- Introduced that the UK Gov were co-funding a research and innovation programme (\$400m) known as Digital Security by Design (DSbD) to investigate potential of CHERI to block vulnerabilities from exploitation
- ARM built the Morello Neoverse N1 prototype SoC, and Microsoft open-sourced CHERIIoT, a RISC-V microcontroller core, both supporting CHERI ISA extensions
- Technology and approach was then investigated internationally...





Cybersecurity is a broad term encompassing the protection of digital systems, networks, and data. This protection aims to prevent unauthorised access, use, disclosure, disruption, modification, or destruction of these assets



Secure by default refers to systems implemented and configured to be secure from the outset. This principle **reduces attack surface** by minimising user intervention in security decisions. Examples include strong default passwords, automatic software updates, formal verification and limiting user privileges



Secure by design is a methodology where security considerations are integrated into every stage of a system's lifecycle, from design to deployment and maintenance. This approach aims to **protect against vulnerabilities**, improved resilience, and lower long-term costs.

Started with
promoting new
terminology...

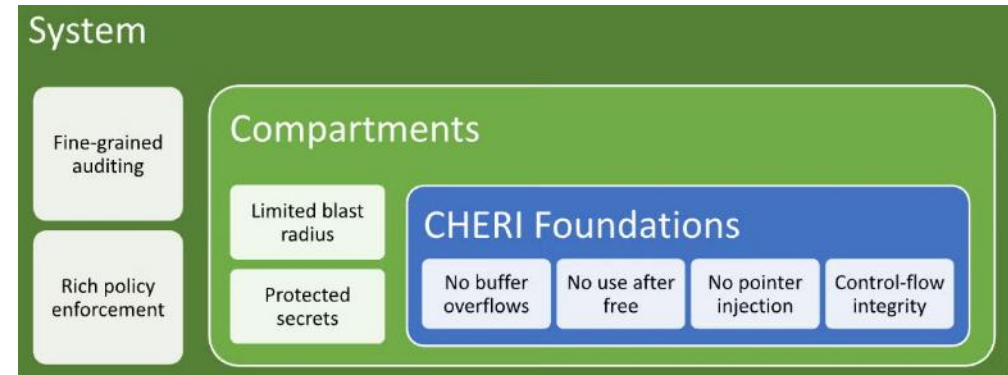
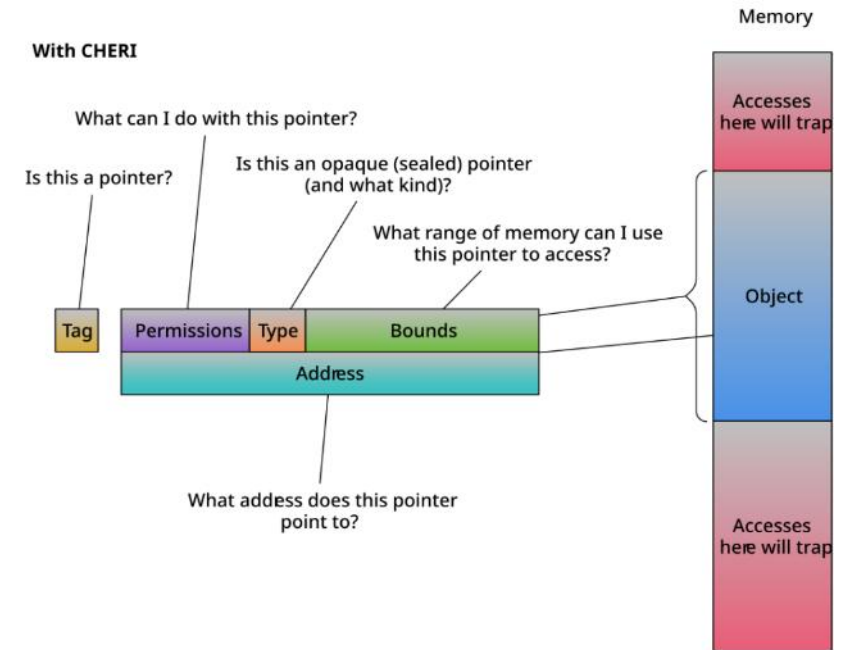
CHERI as a “by design” approach

Capability Hardware Enhanced RISC Instructions (CHERI) is a hardware ISA extension that enforces fine-grained memory protection and enables scalable software compartmentalization.

It replaces pointers with unforgeable capabilities — typically 128-bit tokens on 64-bit systems—that bundle a virtual address with hardware-enforced bounds and permissions, all integrity-protected by a 1-bit memory tag.

This allows for lightweight, hardware-enforced isolation of individual software modules within a single address space by granting them only the minimum necessary capabilities.

On every memory access, the microarchitecture validates the operation against the capability's authority, deterministically mitigating entire classes of vulnerabilities like buffer overflows and control-flow hijacking.



CHERI Fundamentals

Capability-Based: introduces architectural concepts of capabilities, which are unforgeable tokens of authority that control access to memory and resources. This ensures that only authorized code can access specific memory regions.

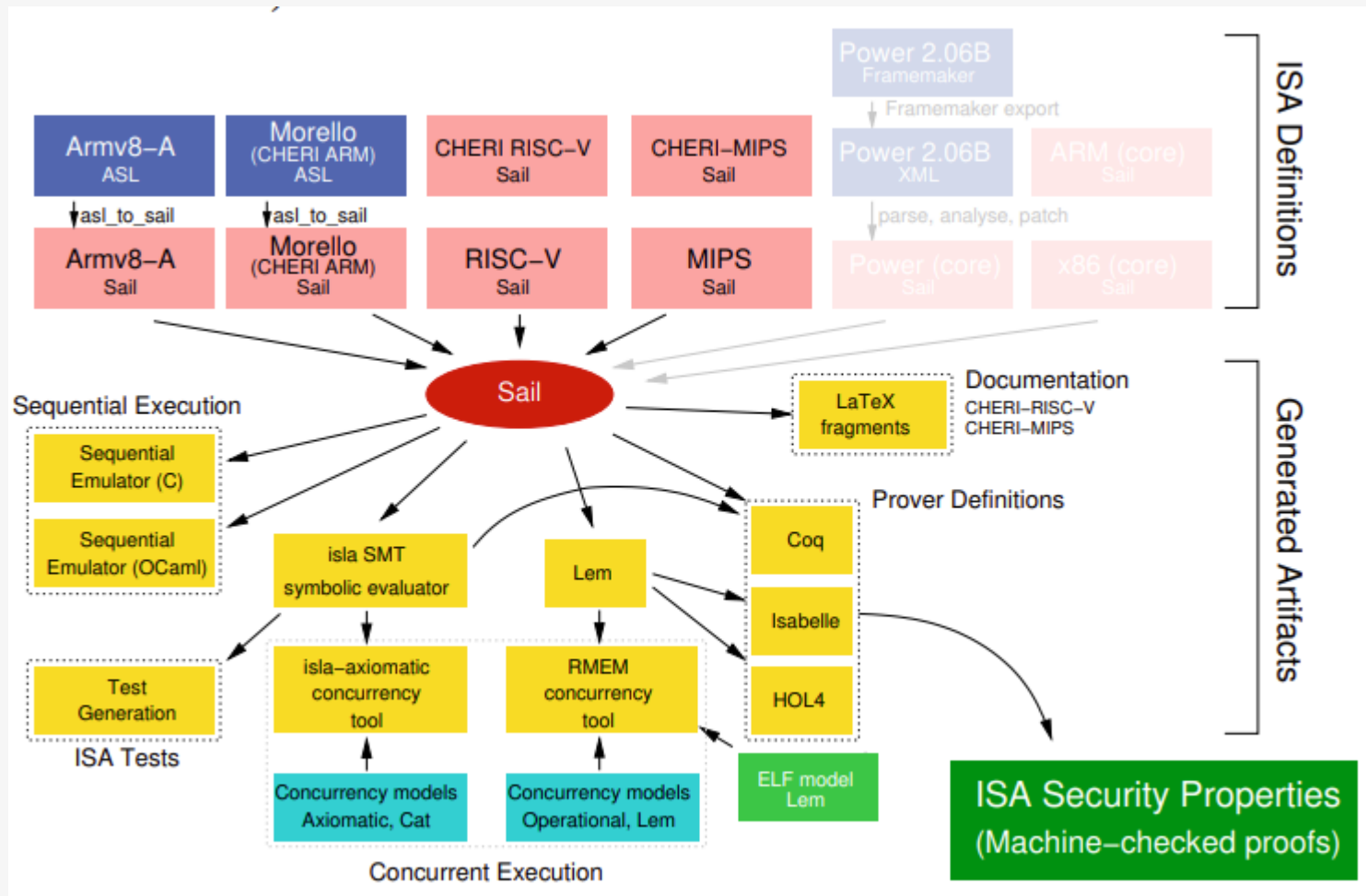
Fine-Grained Memory Protection: provides fine-grained memory protection by associating capabilities with memory addresses.

Compartmentalization: The architecture supports the decomposition of software into isolated compartments. This limits the impact of security vulnerabilities by containing potential exploits within a single compartment.

Provenance and Monotonicity: Capabilities in CHERI enforce strict provenance, meaning they can only be derived from other valid capabilities. They are also monotonic, meaning once restricted, they cannot be broadened again, ensuring that capabilities only become more restrictive as used.

Backward Compatibility: CHERI is designed to be compatible with existing software ecosystems. It allows for incremental deployment within conventional software stacks, enabling a gradual transition to more secure systems.

Formal Verification: CHERI includes formal modeling and verification to ensure that the security properties of the architecture are rigorously defined and maintained

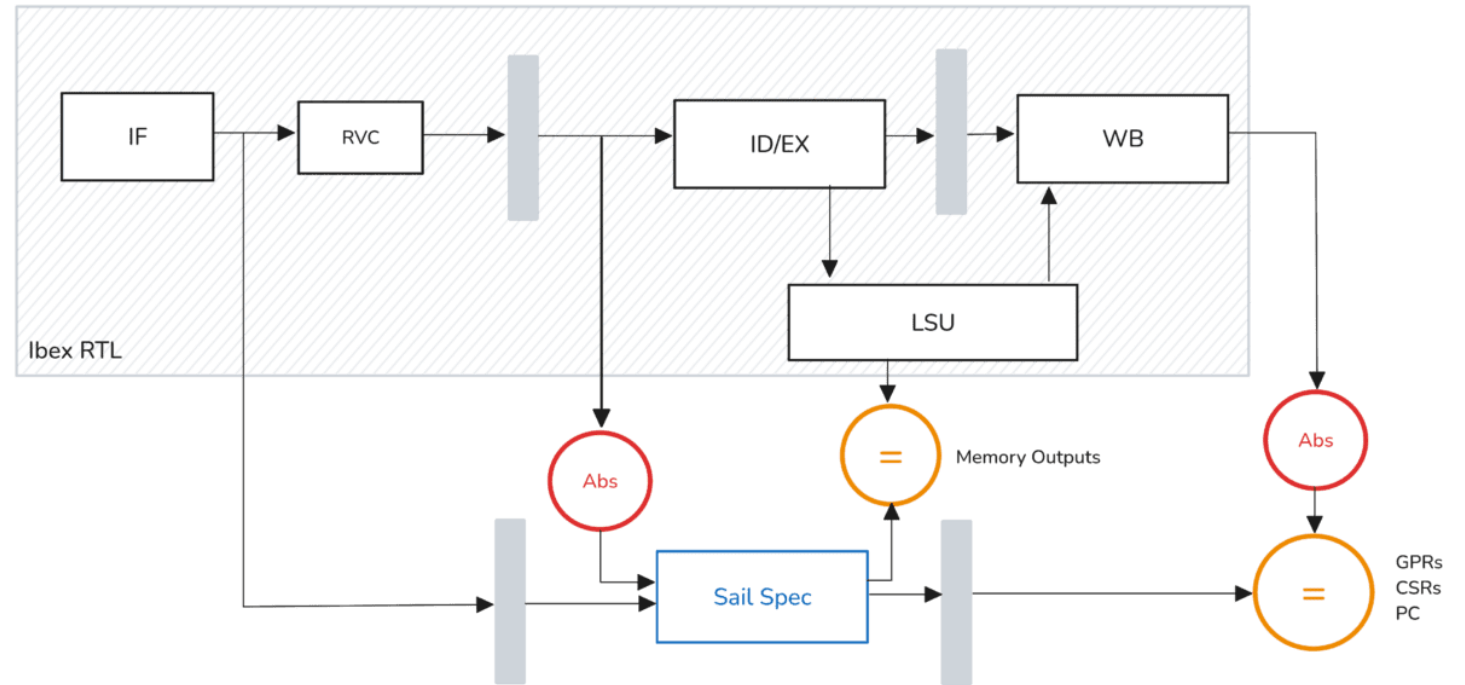


Formal Specification of Hardware Architecture

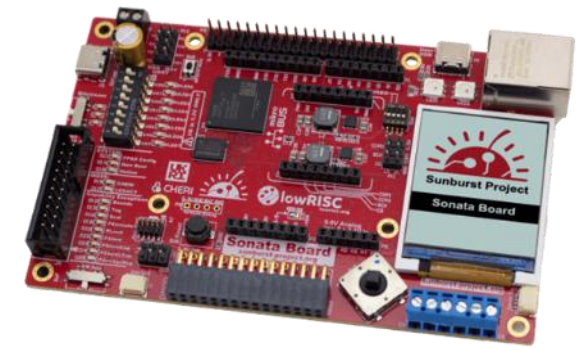
- Arm Morello ISA has a machine-checked mathematical proof of ~60,000 line definition
 - <https://developer.arm.com/documentation/ddi0606/latest/>
- **Engineering with Full-scale Formal Architecture: Morello, Cheri, Armv8-A, and RISC-V**
 - Sewell, P. (2021). Engineering with Full-scale Formal Architecture: Morello, Cheri, Armv8-A, and RISC-V. In Proceedings of the 21st Conference on Formal Methods in Computer-Aided Design – FMCAD 2021 (pp. 12–12). TU Wien Academic Press.

Which led to formal verification of microarchitecture

- Formal verification framework to establish observational equivalence, using **unbounded proofs**, between the hardware and the RISC-V International Sail specification of instruction behaviour



LowRISC Sonata Evaluation System



Sonata is a system for evaluating the usage of Microsoft's CHERIbex core as a microcontroller for embedded, IoT and Operational Technology applications.

The system contains a number of peripherals (I2C, SPI, GPIO, USB, and UART) and the CHERIbex core itself

Commercial (FPGA) dev board

<https://www.mouser.co.uk/new/newae-technology/newae-sonata-one-dev-board>



<https://github.com/lowRISC/sonata-system>

<https://www.mouser.co.uk/new/newae-technology/newae-sonata-one-dev-board/>

..and commercial devices









- Broad base microcontroller applications
- High-efficiency GF 22FDX process
- High integrity and resilient design
- Various RTOS supported, including CHERIOT-RTOS
 - <https://github.com/CHERIOT-Platform/cheriot-rtos>
 - Only a few hundred lines of code within the trusted computing base (TCB)
 - SEL4 ~12k lines and no protections in application space

SCI Semiconductors announce first publicly available CHERI enabled devices.

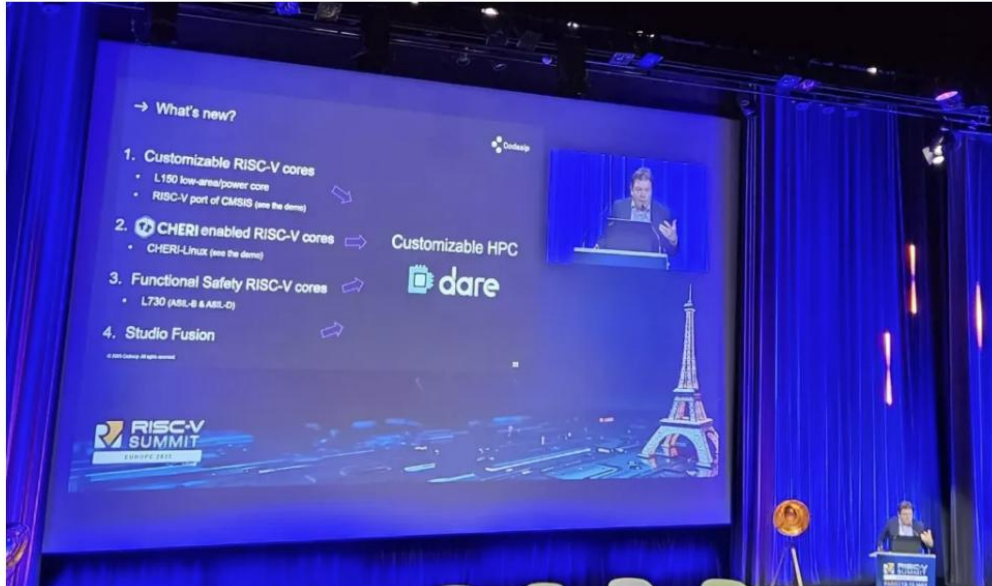
12th August 2024

SCI Semiconductor are very pleased to announce the development of the first commercially available CHERI-enabled family of devices, based on the RISC-V architecture and the Microsoft CHERIOT Ibx processor core. Targeting a wide variety of applications, spanning from Root of Trust (TPM/UICC) through to advanced microcontroller and microprocessor applications, this new family of devices finally delivers CHERI technology as a commercial reality.

The SCI ICENI family of RISC-V (RV32E CHERIOT) microprocessors are specifically designed for applications with high-integrity requirements, including defence and aerospace, critical infrastructure, industry 4.0, and medical domains, although any application where confidential information, control, or command requirements will additionally welcome this protection.

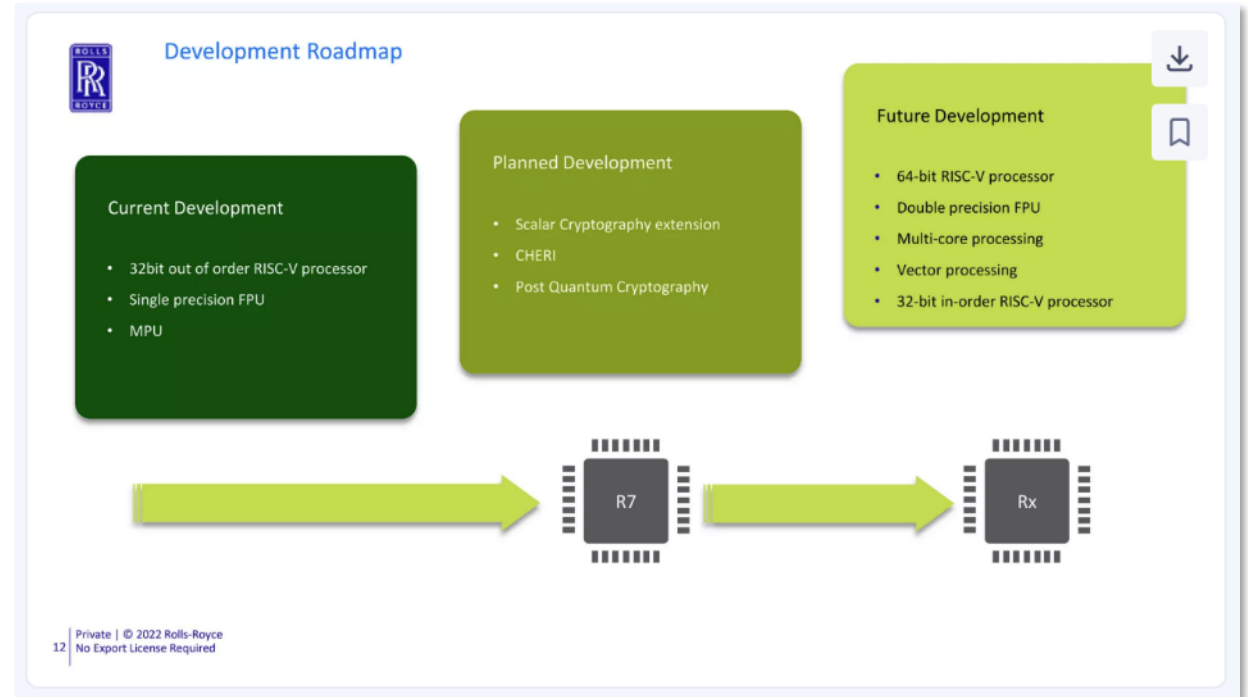
ICENI Family 250MHz+ 32-bit CHERIOT RV32E				JTAG
 Memory Code Up to 2MB MRAM SRAM Up to 1MB ECC SRAM 8KB Data MRAM 8KB	 Analog 12-bit A/D x 10ch Comparator (2ch) Temperature Sensor DAC (2ch) Internal v REF	 Timer 16-Bit Timer Counter (x8) 32-bit Interval Timer (8-bit, 4ch) Watch Dog Timer Unit Real Time Clock	 Protection CHERI Compartmentalisation Capability Memory Safety Security Subsystem* Unique ID MRAM read protection	
 Communication SPI x6 UART x6 Simple I2C x6 I3C* x2 USB x2	 System Capability DMA Integrated System Level Revoker Capability Interrupt Controller Clock Generation Multi On Chip Oscillator Low Power Modes Clock Output TRNG	 Safety SRAM Parity Check SRAM ECC Clock Monitor CRC Independent WDT ADC Self-Test Boot swap (startup area select)	 Package QFN 68, 48, 32, 24 (QFP 68, 48, 32)	

Larger initiatives on the way...



Europe's RISC-V leader to provide a customizable general-purpose processor for the €240M initiative

Munich, Germany, 6 March 2025–Codaip, the European RISC-V leader, announced that it has been selected to provide a general purpose, high-end processor as part of the large-scale European supercomputing project Digital Autonomy with RISC-V in Europe (DARE).



<https://www.slideshare.net/slideshow/developing-future-high-integrity-processing-solutions/253673252#12>

CHERI Alliance

- **Mission:** Be the ISA agnostic industry initiative spearheading the global adoption of CHERI security technology across the computing industry
- **Objective:** Create value for CHERI-enabled products, including processors, development tools, software libraries, chips, and final products and services
- **Collaboration:** Brings together industry leaders, academic institutions, and government bodies to promote the adoption of CHERI technology
- **Education and Support:** The alliance also focuses on educating and supporting software communities and the broader ecosystem to leverage CHERI's security benefits
- **Standardization:** It works towards establishing standards for CHERI technology to ensure widespread and consistent implementation

CHERI Alliance

Driving a global industrial ecosystem to solve the biggest cybersecurity challenge: memory vulnerabilities

Uniting leaders, system developers, users and security experts to drive and promote CHERI as an efficient security standard



Become a
member

Learn
more

<https://cheri-alliance.org/>

Ongoing Government Support



Menu

[Home](#) > [Government](#) > [Cyber security](#) > [CHERI technology for cyber security](#)



Department for
Science, Innovation
& Technology

Policy paper

CHERI technology for cyber security

Published 7 May 2025

Contents

[1. Background](#)
[2. Details](#)


 [Print this page](#)

1. Background

Memory safety bugs in software are repeatedly exploited by hackers to cause major security issues. Research from Google and Microsoft shows that 70% of ongoing cyber vulnerabilities are memory safety bugs. Incidents like the WannaCry attack in 2017 which caused \$4 billion in damages, and the CrowdStrike outage in 2024 which caused a total of \$5.4 billion in direct losses, highlight the severe risks these bugs pose to society, businesses and economies.

Recognising the impact of these costly cyber incidents have been due to memory safety bugs, over £80 million of UK government funding, alongside £200 million of industrial co-investment, has been invested to develop CHERI (Capability Hardware Enhanced RISC Instructions).

<https://www.gov.uk/government/publications/cheri-technology-for-cyber-security/cheri-technology-for-cyber-security>



Innovation Funding Service

Sign in

BETA

This is a new service – your [feedback](#) will help us to improve it.

[Innovate UK](#)

Innovation competitions

Filter competitions

Keywords

Innovation area

Update results

2 competitions

[Contracts for Innovation: DSbD Advancing CHERI Tools and software](#)

• Organisations can apply for a share of up to £12 million, inclusive of VAT, to work on maturing and enabling the availability of CHERI Tools and Software components for RISC-V embedded devices that support the CHERI architecture extensions.

Eligibility
To lead a project you can:

- be an organisation of any size
- work alone or with other organisations as subcontractors

Contracts will be awarded to a single legal entity only.

Closing soon
Opened: 14 May 2025
Closes: 18 June 2025

[Contracts for Innovation: DSbD Advancing CHERI RISC-V Devices](#)

Organisations can apply for a share of up to £10 million, inclusive of VAT, to accelerate the development and implementation of commercial CHERI-enabled RISC-V embedded devices.

Eligibility
To lead a project, you can:

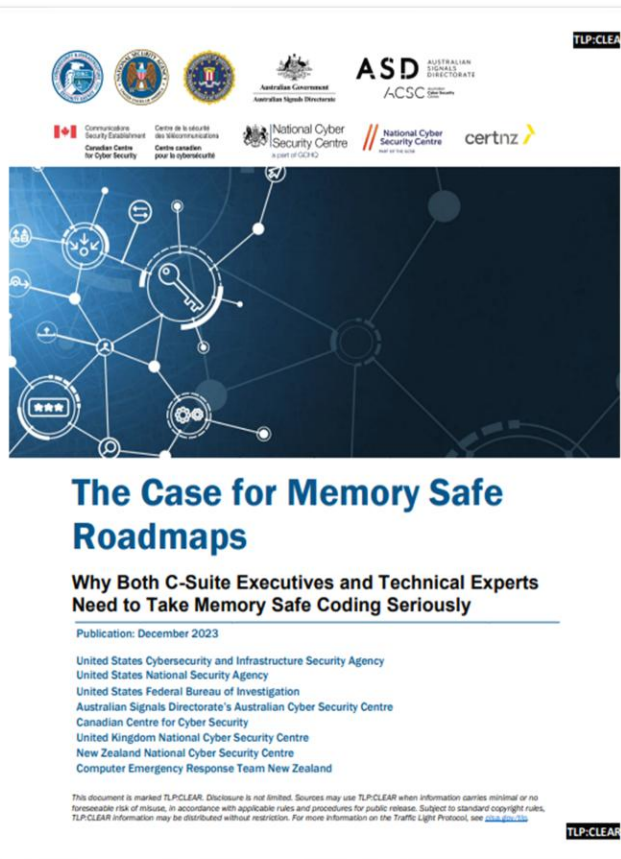
- be an organisation of any size
- work alone or with other organisations as subcontractors

Contracts will be awarded to a single legal entity only.

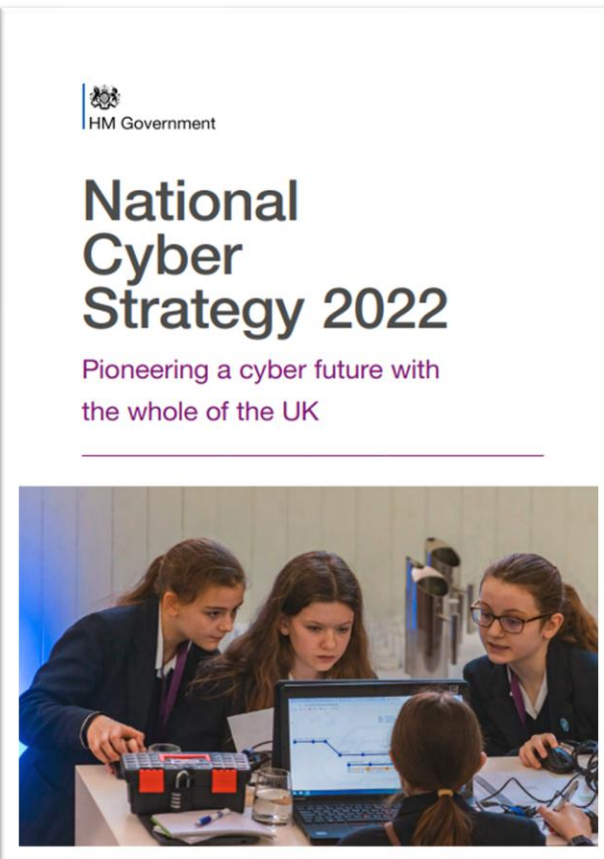
Closing soon
Opened: 14 May 2025
Closes: 18 June 2025

3

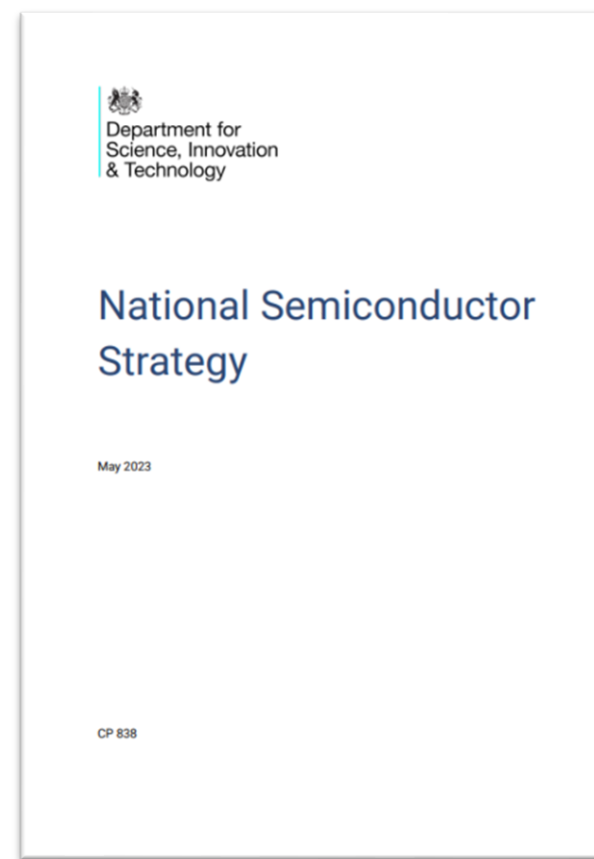
Part of UK and International strategy



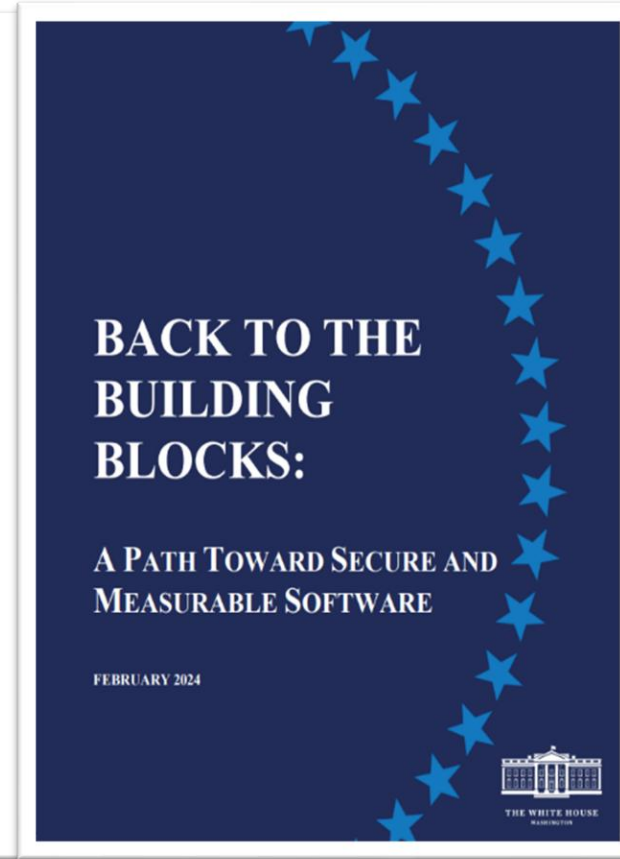
**CISA and 17 International
Cyber Agencies:
Case for Memory Safety**



**UK National Cyber Strategy:
Technology Pillar**



**UK Semiconductor
Strategy**



**Whitehouse
Technical Report**

...USA similarly (as of Dec'24...)



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Secure by Design

- **Early Integration:** Security measures are integrated during the design phase of a product's development lifecycle to significantly reduce exploitable flaws before the product reaches the market.
- **Security as a Core Requirement:** Products designed with secure by design principles prioritize security as a fundamental business requirement, not just a technical feature.
- **Executive Ownership:** Technology providers must take ownership at the executive level to ensure their products are secure by design.



Secure by Default

- **Out-of-the-Box Security:** Products should be secure out-of-the-box, meaning they come with security features enabled by default, such as multi-factor authentication (MFA), logging, and single sign-on (SSO).
- **Ease of Use:** Security features should be easy to use and not require extensive configuration by the end user.
- **Transparency and Accountability:** Technology providers are encouraged to embrace transparency and accountability, making it easier for customers to trust and verify the security of their products.

EU Different: ETSI EN 303 645: IoT Cybersecurity Standard (Shall/Must)

- **Unique or User-Defined Passwords:** Where passwords are used, they ****shall**** be unique per device or defined by the user after the factory default.
- **Secure Password Generation:** Pre-installed unique passwords ****shall**** be generated with a mechanism reducing automated attacks.
- **Best Practice Cryptography for Authentication:** ****shall**** use best practice cryptography.
- **Simple Authentication Value Change:** Users or administrators ****shall**** have a simple mechanism to change authentication values.
- **Brute-Force Attack Prevention:** Non-constrained devices ****shall**** have a mechanism making brute-force attacks via network impracticable.
- **Public Vulnerability Disclosure Policy:** The manufacturer ****shall**** make a vulnerability disclosure policy publicly available.
- **Secure Update Mechanism (Non-Constrained):** Non-constrained devices ****shall**** have an update mechanism for secure installation.
- **Simple Updates:** An update ****shall**** be simple for the user to apply.
- **Best Practice Cryptography for Updates:** The device ****shall**** use best practice cryptography to facilitate secure update mechanisms.
- **Verify Authenticity and Integrity of Network Updates:** Where updates are delivered over a network, the device ****shall**** verify their authenticity and integrity via a trust relationship.
- **Publish Defined Support Period:** The manufacturer ****shall**** publish the defined support period in an accessible way.
- **Recognizable Model Designation:** The model designation ****shall**** be clearly recognizable on the device or via a physical interface.
- **Secure Storage of Sensitive Parameters:** Sensitive security parameters in persistent storage ****shall**** be stored securely by the device.
- **Tamper-Resistant Unique Identity:** Hard-coded unique per device identity for security ****shall**** resist tampering.
- **No Hard-Coded Critical Parameters in Source:** Hard-coded critical security parameters ****shall not**** be used in device software source code.
- **Unique and Securely Produced Critical Parameters:** Critical security parameters for integrity/authenticity checks and secure communication ****shall**** be unique per device and securely produced.
- **Best Practice Cryptography for Communication:** Consumer IoT devices ****shall**** use best practice cryptography to communicate securely.
- **Authenticated Network Access for Configuration Changes:** Device functionality allowing security-relevant configuration changes via network ****shall**** only be accessible after authentication (with exceptions for basic network protocols).
- **Protect Confidentiality of Remote Critical Parameters:** The consumer IoT device ****shall**** protect the confidentiality of critical security parameters communicated via remotely accessible network interfaces.
- **Secure Management Processes for Critical Parameters:** The manufacturer ****shall**** follow secure management processes for critical security parameters.
- **Disable Unused Interfaces:** All unused network and logical interfaces ****shall**** be disabled.
- **Minimize Unauthenticated Disclosure:** In the initialized state, network interfaces ****shall**** minimize the unauthenticated disclosure of security-relevant information.
- **Disable Physically Accessible Debug Interfaces (Software):** Where a debug interface is physically accessible, it ****shall**** be disabled in software.
- **Protect Confidentiality of Sensitive Personal Data:** The confidentiality of sensitive personal data communicated between the device and associated services ****shall**** be protected with appropriate cryptography.
- **Document External Sensing Capabilities:** All external sensing capabilities of the device ****shall**** be documented clearly for the user.
- **Functionality for Simple Data Erasure (Device):** The user ****shall**** be provided with functionality such that user data can be erased from the device in a simple manner.
- **Validate Input Data:** The consumer IoT device software ****shall**** validate data input via interfaces or between networks.
- **Provide Clear Information on Personal Data Processing:** The manufacturer ****shall**** provide consumers with clear and transparent information about processed personal data.
- **Obtain Valid Consent for Personal Data Processing:** Where personal data is processed based on consent, this consent ****shall**** be obtained in a valid way.
- **Capability to Withdraw Consent:** Consumers who gave consent ****shall**** have the capability to withdraw it at any time.

..and then heading towards certifying compliance ¹⁶

DSbD Programme conclusions

- Recompilation of code to CHERI would enable mitigation of 100% of historically reported memory safety vulnerabilities.
- CHERI is a mathematically proven technology that mitigates software memory vulnerabilities through hardware protections
- Targeting of the CHERI architecture unlocks innovation, creating solutions an order of magnitude faster than existing solutions
- Adopting CHERI can be as simple as recompilation with minimal modification
- CHERI can be adopted incrementally without breaking backwards compatibility
- The CHERI extensions are applicable across computer architectures and sectors of the digital market
- The benefits of CHERI can be realised in existing development languages, enabling memory safety for legacy and unsafe code
- Development tools and compilers have reached a level of maturity that enable early commercial adoption
- CHERI-based architectures provide formal modelling and software verification tools with additional semantics to accelerate and improve the accuracy of software verification
- CHERI enables high performance compartmentalisation of code
- CHERI strengthens the operating foundations of computing.
- DSbD ecosystem has demonstrated that the most complex and ubiquitous system software can benefit from the use of CHERI
- The concepts of CHERI and secure by design have stimulated an international response and the frameworks necessary for aligned response
- Some business practices, methodologies and broader governances, especially for safety-critical systems can lead to non-obvious barriers to the adoption of CHERI



Digital Security by Design (DSbD) programme outcomes:

Evidential claims for the CHERI technology across DSbD project investigations



Adopting CHERI memory-safe hardware extensions will:
Reduce business costs | Enhance user and developer experience
Strengthen digital security and resilience

<https://www.ukri.org/wp-content/uploads/2025/06/IUK-030625-DigitalSecurityDesignProgrammeOutcomes.pdf>

More info:

- Useful Links
 - <https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/>
 - <https://cheriot.org/>
 - <https://github.com/lowRISC/sunburst-chip>
- Alliance of CHERI adopters and implementors
 - <https://cheri-alliance.org/>
- Commercially available RISC-V IP and devices
 - <https://cudasip.com/solutions/riscv-processor-safety-security/cheri/>
 - <https://www.scisemi.com/>
 - <https://www.secqai.com/our-products/soc>
- Standardization work in RISC-V International
 - <https://github.com/riscv/riscv-cheri>