The CHERI Research Centre (CRC)

Professor Robert N. M. Watson
University of Cambridge, CHERI Alliance, and Capabilities Limited

CHERI Blossoms Conference
University of Cambridge
26-27 March 2026

Approved for public release; distribution is unlimited.

Development of the CHERI concept was supported by the **Defense Advanced Research Projects Agency (DARPA)** and the Air Force Research Laboratory (AFRL), under contract FA8750-10-C-0237 ("CTSRD"), with additional support from FA8750-11-C-0249 ("MRC2"), HR0011-18-C-0016 ("ECATS"), FA8650-18-C-7809 ("CIFV"), HR001122C0110 ("ETC"), HR001123C0031 ("MTSS"), and FA8750-24-C-B047 ("DEC") as part of the DARPA I2O CRASH, I2O MRC, MTO SSITH, and I2O CPM research programs. The views, opinions, and/or findings contained in this document are those of the authors and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Arm's Morello and the Morello-enabled software stack, as well as development of the RV64Y Instruction-Set Architecture (ISA) standard, were supported by the **Innovate UK** projects 105694 ("Digital Security by Design (DSbD) Technology Platform Prototype"), 107145 ("Assessing the Viability of an Open-Source CHERI Desktop Software Ecosystem"), 10027440 ("Developing and Evaluating an Open-Source Desktop for Arm Morello"), 10027332 ("MOJO - A Robust Java Virtual Machine for Morello"), 10168042 ("CheriBSD feature extraction, maturity, and testing), and 10168492 ("CHERI for Operational Safety in Memory-Isolated Cores").

Research from 2025 was supported primarily by the **DSIT and EPSRC** CHERI Research Centre (CRC) grant UKRI3001.

We further acknowledge EPSRC REMS (EP/K008528/1), EPSRC CHaOS (EP/V000292/1), ERC ELVER (789108), the Isaac Newton Trust, the UK Higher Education Innovation Fund (HEIF), Thales E-Security, Microsoft Research Cambridge, Arm Limited, Google, Google DeepMind, HP Enterprise, Codasip, and the Gates Cambridge Trust.

Gratefully acknowledging many papers, reports, and talks co-authored with members of the CHERI Research Project since 2010 …

Simon W. Moore, Peter Sewell, Peter G. Neumann, and **Brooks Davis**

Hesham Almatary, Ricardo de Oliveira Almeida, Jonathan Anderson, Alasdair Armstrong, Rosie Baish, Peter Blandford-Baker, John Baldwin, Hadrien Barrel, Thomas Bauereiss, Ruslan Bukin, Brian Campbell, David Chisnall, Jessica Clarke, Kian Cross, Nirav Dave, Lawrence Esswood, Nathaniel W. Filardo, Franz Fuchs, Dapeng Gao, Ivan Gomes-Ribeiro, Khilan Gudka, Brett Gutstein, Angus Hammond, Graeme Jenkinson, Alexandre Joannou, Mark Johnston, Robert Kovacsics, Ben Laurie, Ka Wing Li, Zhuo Ying Jiang Li, Jessica Man, A. Theo Markettos, J. Edward Maste, Alfredo Mazzinghi, Paul Metzger, Alan Mujumdar, Prashanth Mundkur, Steven J. Murdoch, Edward Napierala, George Neville-Neil, Kyndylan Nienhuis, Robert Norton-Wright, Philip Paeps, Lucian Paul-Trifu, Allison Randal, Ivan Ribeiro, Alex Richardson, Michael Roe, Colin Rothwell, Peter Rugg, Hassen Saidi, Thomas Sewell, Stacey Son, Ian Stark, Domagoj Stolfa, Andrew Turner, Munraj Vadera, Qianhui Wang, Yuecheng Wang, Konrad Witaszczyk, Jonathan Woodruff, Hongyan Xia, Vadim Zaliva, and Bjoern A. Zeeb

University of Cambridge, SRI International, Capabilities Limited, Arm, Google, Microsoft, lowRISC, MSB, Ararat, and SCI Semi

A little bit of history

- Founded in 2010, supported by DARPA, the **CHERI Research Project** has been tasked with developing new techniques to fundamentally transform computer security, reconsidering the full hardware-software stack.
- The collaboration began with the **University of Cambridge** and **SRI International** – but now is an international collaboration supported by investment >$300M from the US/UK governments and industry, including collaborators such as **Arm**, **Ericsson, Capabilities Limited, Codasip, Google**, **lowRISC**, **Microsoft**, **SCI Semi**, **SECQAI**, and many others.
- There is new a **rapidly growing ecosystem** of organisations building CHERI-based hardware, adapting software to CHERI, and integrating CHERI into first generation products – and need support in doing so!

What is the CHERI Research Centre (CRC)?

The goals of the CHERI Research Centre, created in 2025, are to:

1. Support industrial, academic, and government communities adopting CHERI by addressing gaps in research, standards, and education/training
2. Directly engage with the development of third-party CHERI-enabled products, working side-by-side with hardware and software teams at industrial and other partners
3. Develop and maintain open-source reference designs, documentation, … to accelerate adoption

The starting point for the CHERI Research Centre was the existing hardware-software-theory team at the University of Cambridge with unique cross-layer and CHERI expertise:

- The 30+-member team spans security, architecture, systems, programming languages, and theory research groups in the department, as well as collaborators at SRI and CapLtd
- Around a dozen are PhD students working on CHERI across hardware, software, and theory

Primary support by a grant from DSIT / EPSRC

Additional support from DARPA and industrial sponsors, especially for PhD students

Critical question: Where is there still research to do?

Transitioning CHERI to industrial use demands a strong academic-focused team blending research and engineering, working alongside industry:

- **Fundamental research** – Disruptive improvements to the CHERI model in hardware and/or software (e.g., temporal safety, integration with I/O, heterogeneous accelerators) and new software use (e.g., compartmentalization models and use at scale)
- **Applied research** – Evaluating at scale + analysing behavior/ performance, enabling adoption (e.g., optimising memory footprint / compiler, creating open-source hardware-software reference designs)
- **Standards and best practices development** – Downselecting, optimizing, and refining CHERI from Arm Morello to RVY (e.g., compartmentalization, temporal safety), developing memory-safety definitions and assurance levels, and developing guidance on CHERI hardware and software best practices

Some of our areas of ongoing research

- We now have **very large-scale experience with CHERI C/C++ memory safety** (>200MLoC of open-source software) – **what lessons can we learn** from that about the practical deployment of memory safety, and can we further improve our approach?
- CHERI was designed to support C/C++ memory safety and compartmentalization – but some of our most critical, and most vulnerable, TCBs are **language runtimes for high-level and managed languages**. How could CHERI help .. and will we need to change CHERI to do that?
- CHERI's scalable compartmentalization primitives open the door for vulnerability mitigation far beyond memory safety – but what are the **accessible software compartmentalization models** enabled by CHERI, and what new engineering practices and tooling will be required to make this useful "at scale" in major software ecosystems?
- CHERI has been designed for general-purpose CPUs running commodity instruction sets, but **specialised cores and accelerators** are now critical to power and performance. How can CHERI integrate with GPUs, NPUs, and other accelerators to provide consistent strong protection across a full SoC?
- How can we help government + industry express strong **demand signals for memory safety and compartmentalization** through technical contributions, standardization, and outreach?

Research: Temporal safety for application cores

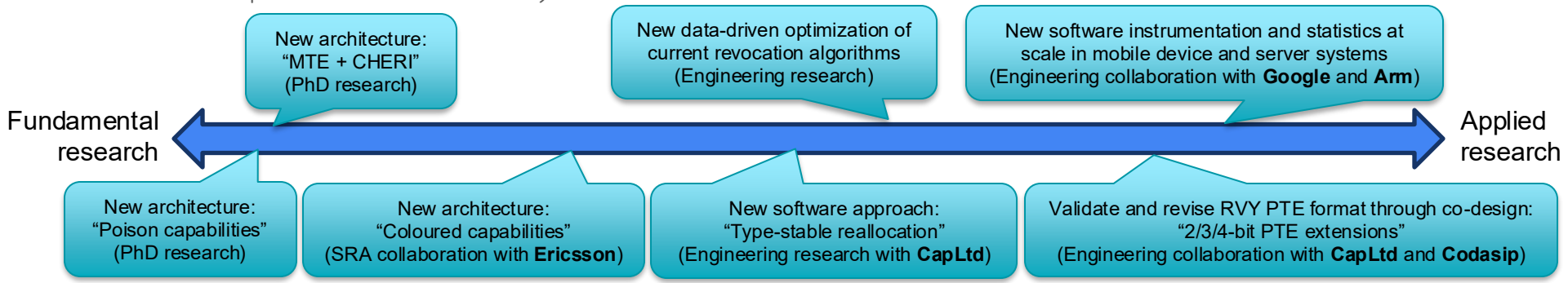
Temporal memory safety prevents exploitation of use-after-free vulnerabilities (~50% of memory-safety vulnerabilities) – and is essential to scalable compartmentalisation:

- Revocation can be **centralized but unscalable** or **decentralized and scalable**
- Contemporary microarchitecture demands decentralization – creating significant challenges
- Over 4 papers and 2 PhDs (2019-2024) we proposed using **sweeping revocation**

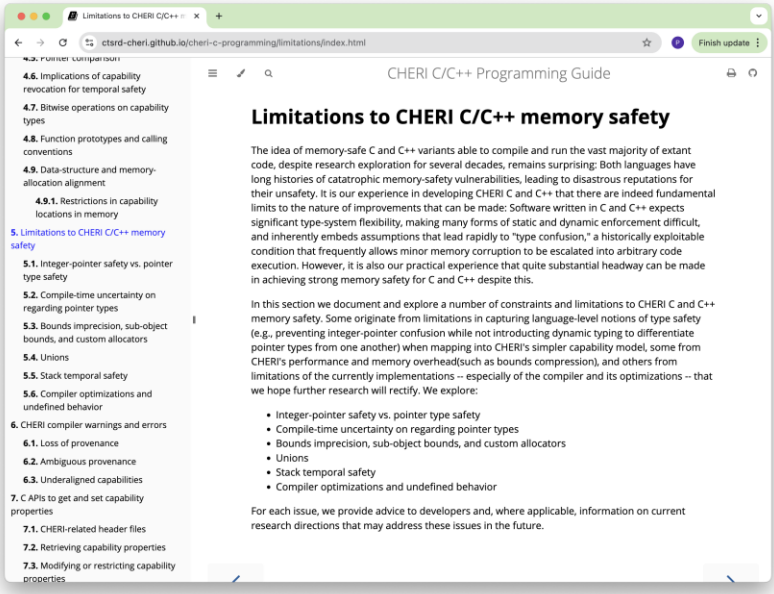
Industrial RVY development have so far focused on (easier) spatial safety (the other ~50%)

- Memory and performance overheads for some workloads exceed industry tolerance (10% > 2%)
- Draft specification contained serious errors due to lack of full HW-SW validation

We performed several pieces of work from delivering currently understood techniques (matured using extensive experience from Morello) to novel HW-SW research:



Communications: Documenting CHERI limitations

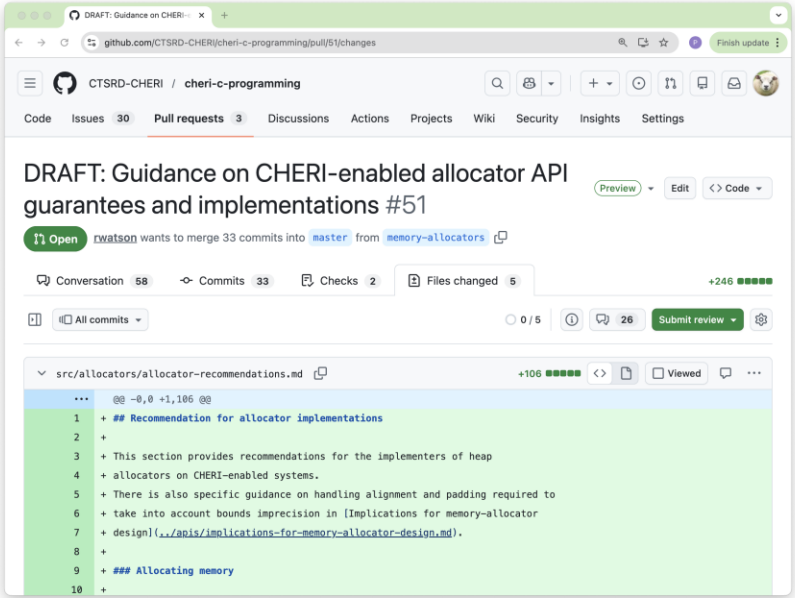


As with all technologies, CHERI has important limitations to what it can achieve:

- Potential adopters need to use that information to evaluate costs and benefits of adoption
- Users of CHERI-enabled products need to understand those limitations to use it safely and effectively
- Documentation of limitations is **essential** to the credibility of CHERI as a technology
- In collaboration with industrial partners, we have **developed new documentation of CHERI limitations** as part of an updated CHERI C/C++ Programming Guide

This work was performed in collaboration with Arm, Bloomberg, CapLtd, Codasip, Google, and SCI Semi.

Communications: Documenting software best practices

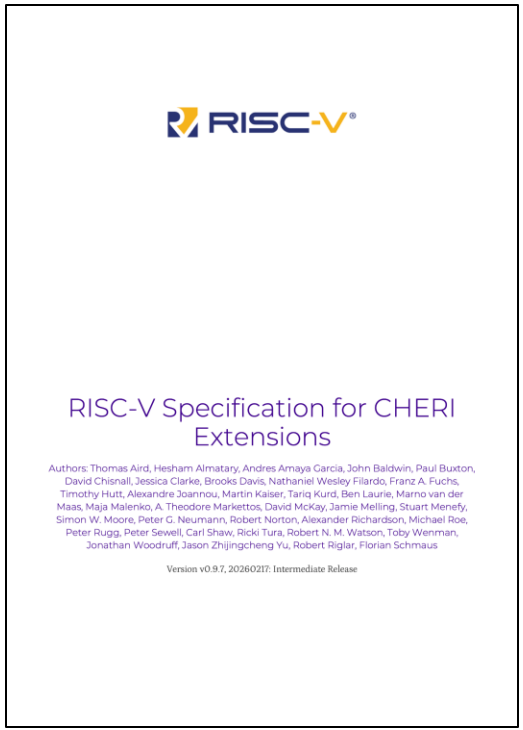


Correct implementation of software Trusted Computing Bases (TCBs) is essential to safe use:

- **Memory allocators** provide memory-allocation information to CHERI hardware
- In collaboration with industrial partners, **developed memory-allocator best practices** applicable from microcontrollers (e.g., CHERIoT) through to application cores (e.g., Morello, X730)
- E.g., **In-progress text** in the CHERI C/C++ Programming Guide documents how to use and implement memory allocators safely

This work has been in close collaboration with Arm, CapLtd, Codasip, Google, SIFT, and SCI Semi.

Successful activities drawing to a close for Year 1


RISC-V

RISC-V Specification for CHERI Extensions

Authors: Thomas Aird, Hesham Almatary, Andres Amaya Garcia, John Baldwin, Paul Buxton, David Chisnall, Jessica Clarke, Brooks Davis, Nathaniel Wesley Filardo, Franz A. Fuchs, Timothy Hutt, Alexandre Joannou, Martin Kaiser, Tariq Kurd, Ben Laurie, Marno van der Maas, Maja Malenko, A. Theodore Markettos, David McKay, Jamie Melling, Stuart Menefy, Simon W. Moore, Peter G. Neumann, Robert Norton, Alexander Richardson, Michael Roe, Peter Rugg, Peter Sewell, Carl Shaw, Ricki Tura, Robert N. M. Watson, Toby Wenman, Jonathan Woodruff, Jason Zhijingcheng Yu, Robert Riglar, Florian Schmaus

Version v0.9.7, 20260217: Intermediate Release

Open-source hardware and software reference designs:

- **RVY-compliant CHERI-Toooba** research processor design
- **RVY-compliant open-source software** including CHERI LLVM compiler, CHERI GDB debugger, CheriBSD OS, and seL4 OS

Standards and compliance contributions:

- **RISC-V International "CHERIv1"** – RVY extension approaching ratification, which will enable a first generation of standards-compliant cores (e.g., Codasip X730 and CapLtd CVA6-CHERI) and software – in extensive collaboration with Codasip, Google, SCI Semi, and others
- **ETSI memory-safety definitions** – Early draft "Memory-safety definitions and assurance levels" in CapLtd/NCSC-led effort within ETSI

New activities ramping up in Year 2

Examples of new communication and education activities:

- **New CHERI Seminar Series** (joint with CHERI Alliance) in Cambridge and online
- **New CHERI education material**
  - **Undergraduate education material** for use by UK/international universities
  - **Pre-university education material** for use by UK/international schools

Examples of open-source hardware and software activities:

- Support maturity of **"second source" open-source application-core IP** based on CapLtd's CVA6-CHERI, in collaboration with lowRISC + Oxford, to addressing industrial hardware IP supply-chain resilience
- Contribute to **maturing CHERI Linux** alongside industrial partners, contributing to open-source specifications and test suites led by CRC
- Support **open-source CHERI reference "computer design"**, an FPGA-based design based on CapLtd's CVA6-CHERI, illustrating a "full computer" (including I/O / DMA) as a continuing foundation for research, demonstrators, and products in industry and academia

Do reach out with any questions, and see you around the conference!