Delivered by Innovate UK,
EPSRC and ESRC

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

Introduction

The DSbD programme outcomes across project investigations have demonstrated that adopting the Capability Hardware Enhanced RISC Instructions (CHERI) technology can significantly benefit businesses by reducing cyber related costs and bolstering digital security and resilience.

CHERI achieves this by effectively mitigating software vulnerabilities, a major source of security risks and expenses. As reported across ecosystems ranging from embedded to server, typically 70% of total reported vulnerabilities stem from memory safety errors. The DSbD programme, through the recompilation of large software corpuses totalling millions of lines of legacy code, has shown that CHERI could have prevented 100% of these previously identified memory safety vulnerabilities, significantly enhancing national cyber-defence capabilities.

CHERI technology is remarkably versatile, applicable across diverse sectors and computer architectures. It requires minimal code adaptation and seamlessly integrates with existing development languages and toolchains. This enables a smooth, incremental adoption process without disrupting existing systems, allowing organisations to prioritise security enhancements where they are most critical.

At the heart of CHERI's security model is its ability to enhance security across all layers of the computing stack, from the foundational RTOS, operating systems, unikernels and hypervisors to applications and even AI technology stacks. This comprehensive approach facilitates the creation of formally provable trusted code bases, establishing auditable trust relationships with the supply chain. CHERI's robust isolation between components effectively blocks the escalation of errors, ransomware and protection of sensitive data from leakage and exfiltration.

Furthermore, CHERI's innovative approach to security has fostered international collaboration and associated traction towards the adoption of CHERI and secure-by-design principles globally. This collaborative effort underscores the growing recognition of CHERI's transformative potential in shaping a more secure and resilient digital future.

Based on the analysis of the ecosystem-wide range of reports, papers and outputs of the DSbD projects and related investigations, we find evidence to support the claims for CHERI that on its course to adoption the following benefits are realised.

CHERI reduces Business Costs

- **Claim #1: Recompilation of code to CHERI would enable mitigation of 100% of historically reported memory safety vulnerabilities.** This directly addresses the financial burden of addressing security vulnerabilities. Analyses across multiple software ecosystems have shown that typically an average of 70% of total ongoing vulnerabilities are due to memory safety issues. Subsequent analyses have shown that 70% to 100%, of these memory safety vulnerabilities would have been mitigated and blocked from exploitation by CHERI, depending on the software package. By mitigating vulnerabilities, CHERI would reduce spending on reactive security measures such as patch development. This has been described as costing 7% per developer in productivity. Also, it has been shown that UK businesses, on average, are spending $1.4M a year on preventing, detecting and remediating vulnerabilities.

- **Claim #2: CHERI is a mathematically proven technology that mitigates software memory vulnerabilities through hardware protections.** CHERI's mathematical foundations suggest decreased costs associated with fixing vulnerabilities, as well as a reduced likelihood of costly security incidents documented at around a £27 billion loss to UK businesses in 2023.

- **Claim #3: Targeting of the CHERI architecture unlocks innovation, creating solutions an order of magnitude faster than existing solutions.** CHERI's potential to create faster solutions presents opportunities for competitive advantage and reduced energy consumption. The project outcomes explain that existing isolation mechanisms are costly due to their reliance on inefficient context-switching and data movement. CHERI addresses this by introducing the concept of compartmentalisation, simplifying data transfer and reducing overheads

CHERI enhances User and Developer experience

- **Claim #4: Adopting CHERI can be as simple as recompilation with minimal modification.** Across various sectors, porting legacy software to CHERI adds memory safety and requires minimal software changes (lines-of-code), ranging from 1-2% to less than 0.1% code modification. This minimal change suggests that CHERI can be incorporated into existing projects without significant disruption or cost, resulting in enhanced end-user experience due to higher resilience and less need to patch. One small university team adapted over 150MLoC of existing C/C++ code to memory safety — a remarkably productivity rate.

- **Claim #5: CHERI can be adopted incrementally without breaking backwards compatibility.** This incremental adoption allows organisations to transition to CHERI at their own pace. On higher-end mobile and server systems, legacy applications can run side-by-side with CHERI-protected applications. Minimally, recompilation is required as operating systems and RTOS gradually integrate CHERI to become memory safe. The costs of adopting the new technology can therefore be managed by technology companies by targeting efforts into key areas without having to invest everywhere.

- **Claim #6: The CHERI extensions are applicable across computer architectures and sectors of the digital market.** CHERI implementations exist in architectures ranging from microcontrollers to server-class devices. CHERI's broad applicability simplifies integration and access to skilled workers. It has also been evaluated for inclusion in the Intel/AMD (x86) architecture due to its non-assertive openly available IP policy. This wide applicability minimises the need for specialised expertise for different environments.

- **Claim #7: The benefits of CHERI can be realised in existing development languages, enabling memory safety for legacy and unsafe code.** CHERI has been shown to benefit a variety of both legacy and memory safe development languages, including C/C++, Java, Rust, WebAssembly, JavaScript, Ada, and Python. This broad support allows developers to utilise CHERI without learning a new language or extensively rewriting existing code, removing barriers and ensuring a standardised low-risk route to adoption.

- **Claim #8: Development tools and compilers have reached a level of maturity that enable early commercial adoption.** The maturity of key tools and compilers, like GCC and LLVM, demonstrate an increasingly established ecosystem for CHERI development. This allows developers to begin building CHERI-based solutions with relative ease.

- **Claim #9: CHERI-based architectures provide formal modelling and software verification tools with additional semantics to accelerate and improve the accuracy of software verification.** CHERI provides extra information about memory manipulation to software verification tools, leading to faster and more accurate verification. This streamlines the development process by helping developers to identify and address potential issues more effectively resulting in higher integrity and resilient solutions.

CHERI strengthens digital security and resilience

- **Claim #10: CHERI enables high performance compartmentalisation of code.** In addition to memory safety, CHERI provides mechanisms for fine grained isolation in which code operates on a need-to-know basis, a strict relationship for sharing and recoverability of failure, increasing resilience of solutions.

- **Claim #11: CHERI strengthens the operating foundations of computing.** It delivers increased security across the real-time operating systems (RTOS), platform and unikernel OS and hypervisors landscape.

- **Claim #12: DSbD ecosystem has demonstrated that the most complex and ubiquitous system software can benefit from the use of CHERI.** The integration of CHERI into complex system software like the Java Virtual Machine (JVM), WebAssembly Micro Runtime (WAMR), open-source desktop environment, and web browsers ensures that vital and complex applications can also benefit from CHERI's security enhancements.

- **Claim #13: The concepts of CHERI and secure by design have stimulated an international response and the frameworks necessary for aligned response.** Growing international recognition of CHERI, including by organisations like CISA and the White House, signals a collaborative effort to build a more secure digital landscape. Global collaboration is crucial for addressing the international nature of cyber security and associated supply chain challenges.

- **Claim #14: Some business practices, methodologies and broader governances, especially for safety-critical systems can lead to non-obvious barriers to the adoption of CHERI.** CHERI's introduction of defined behaviour to areas previously undefined in computer systems would potentially conflict with existing development methodologies, regulated practice and liability in safety-critical markets. Once these non-technical barriers are understood, CHERI will be able to reduce the cost and impact of needing to manage otherwise undefined system behaviour leading to safer systems.

DSbD Corpus of Evidence

All the claims in this document have been extracted from the corpus of project outputs generated during the DSbD programme 2019-2025. This categorises the above 14 claims against a narrative and supporting evidence.

The corpus of project outputs will be available as a publication under the Outcomes and Impacts section of the DSbD website and will be updated as further papers are published.

For more information visit dsbd.tech