CHERI Alliance Officially Launches, Adds Major Partners including Google, to Tackle Cybersecurity Threats at the Hardware Level

Tuesday 12 November, 2024

Founding members include global commercial, research, and open-source organizations, and several UK universities and government entities

CAMBRIDGE, the United Kingdom – November 12, 2024 – The CHERI Alliance CIC (Community Interest Company) today announced its official launch and the expansion of its membership, welcoming Chevin Technology (UK), Critical Technologies (USA), the Defence Science and Technology Laboratory (DSTL, UK), Google (USA), Light Momentum Technology Corporation (Taiwan), National Cyber Security Centre (NCSC, a part of GCHQ, UK), Parvat Infotech (India), SRI International (USA), TechWorks (UK), Trusted Computer Center of Excellence (USA), the University of Birmingham (UK), and the University of Glasgow (UK) as founding members.

Founded to unite hardware security leaders and system developers, the CHERI Alliance aims to establish CHERI (Capability Hardware Enhanced RISC Instructions) as the new standard for memory safety and scalable software compartmentalization.

Previously announced founding members of the CHERI Alliance include Capabilities Limited, Codasip, CyNam, the FreeBSD Foundation, lowRISC, OpenHW Group, SCI Semiconductor, Swansea University, and the University of Cambridge. Following its initial formation in June 2024, the CHERI Alliance's new additions reinforce the collaborative effort to protect against memory-related vulnerabilities, a critical security challenge that constitutes approximately 70% of the vulnerabilities exploited in cyberattacks.

"Expanding our membership signals growing recognition of CHERI's transformative potential," said **Dr. Robert N. M. Watson, Professor, University of Cambridge, Director of the CHERI Alliance, and Director of Capabilities Limited**. "After more than a decade of development, it's rewarding to see the CHERI community grow as new members bring their innovation and commitment to the Alliance. We are now well-positioned to advance our mission of delivering scalable, hardware-based security solutions that address critical vulnerabilities."

UK Minister for AI and Digital Government Feryal Clark said: "Digital and online security is a fundamental part of our duty as a government to keep the British public, our vital services, and our critical national infrastructure safe. CHERI is a fantastic example of how brilliant British ingenuity is rising to that challenge, focusing on shoring up our defences in areas which are so often a target for would-be cyber attackers. It's great to see our national security community and some of the leading lights in tech backing this work – ensuring a joined-up approach which will keep our digital economy and the services we rely on daily safe, secure, and alert to the growing range of online threats that we face."

CHERI technology, developed starting in 2010 through a collaboration between the University of Cambridge and SRI International, offers robust protection against memory safety issues such as buffer overflows and heap use-after-free vulnerabilities. The technology's ability to enable high-performance, scalable compartmentalization significantly reduces the risk of both known and future unknown vulnerabilities.

With a broader range of companies, open-source organizations, and research institutions on board, the CHERI Alliance is poised to strengthen its efforts in standardization, technical alignment, and educational outreach to promote CHERI's adoption as an industry-standard security measure.

Supporting Quotes from New Alliance Members

Ben Laurie, Lead Security Researcher at Google, commented: "Google's interest in CHERI stems from our unwavering commitment to security and privacy. We recognize the potential of CHERI in significantly enhancing system security by mitigating common software vulnerabilities. CHERI offers fine-grained compartmentalisation, which isolates sensitive data into secure compartments, and deterministic memory safety. In security-critical systems that handle sensitive information and personal data, such as those found in generative AI applications, CHERI helps protect against breaches and ensures robust protection against malicious attacks."

Media:

Related Sectors:

Computing & Telecoms :: Consumer Technology :: Government :: Manufacturing, Engineering & Energy ::

Related Keywords:

Cybersecurity :: CHERI :: Memory Safety :: Technology :: NCSC :: DSIT :: DSTL ::

Scan Me:

Stuart W. Card, VP & Chief Scientist, Critical Technologies, said: ”Critical Technologies Inc. (CTI) designs to integrate Capability Hardware Enhanced RISC Instructions (CHERI), driven by the CHERI Alliance, into open platforms for *trustworthy networked autonomy*. With Syracuse University, CTI previously developed the first (and still to our knowledge only) capability based, formally verified, open source, multiboot loader for x86 processors with ‘late launch’ DRTM instructions and TPMs; we will do likewise with CHERI as needed to enable seL4® based virtualization for safe AI/ML.”

Allen Cheng, CEO of LMT, said: “LMT is excited to join the CHERI Alliance and contribute to a future of enhanced security and reliability in computing. Our commitment to providing dependable computing solutions aligns perfectly with CHERI's vision of a safer digital landscape. We look forward to leveraging CHERI technology to develop innovative and secure IC products and services. As a CHERI ambassador in Taiwan and the APAC region, we will actively promote this cutting-edge technology to industry leaders, agencies, and associations, addressing the growing cybersecurity challenges posed by today's geopolitical climate.”

Dr. Divya Atkins, co-founder, Director, and CEO of Parvat Infotech, said: “CHERI is a transformational technology, but until now has been largely limited to the UK. We want to see its advantages extended to the rest of the world, and especially to India, where, at one end of the spectrum, there is a vast digital public infrastructure using server class hardware, and at the other end, smart cities full of IoT devices. All of these need better security, and our goal is to make that happen. Parvat, being an Indian company, is a newcomer to CHERI, but our principals have been working with CHERI in the UK, so we have the knowledge and experience to support our goal, as well as the mission of the CHERI Alliance.”

Patrick Hurley, TCCoE Executive Director, said: “Trusted Computing Center of Excellence (TCCoE) members are eager to work with CHERI Alliance members to foster trustworthy foundations for computing. CHERI Alliance driven standard hardware support for efficient memory access capabilities complements TCCoE facilitated and promoted formal methods for development and verification of operating systems and other software. These synergistic techniques offer a path out of the current crisis in the safety/security/complexity of software dependent systems to a more resilient and prosperous future.”

John Moor, COO, TechWorks, said: “The challenge of memory safety is a significant and growing problem for computing and cybersecurity – it simply cannot be ignored. Industry must provide solutions for this challenge as the world becomes increasingly digital and connected. As the UK’s deep tech trade association, we understand the power of collaboration and TechWorks is fully supportive of the CHERI Alliance and its ambitious goals. We look forward to working with the CHERI Alliance to help raise more awareness and enable more commercially-available memory-safe solutions.”

Jeremy Singer, a Reader in Programming Language Implementation at the School of Computing Science, University of Glasgow, said: “We are delighted to join the CHERI Alliance, since we are actively contributing CHERI patches to open-source codebases and we want to do all we can to encourage wider adoption of memory safe compute platforms like CHERI.”

Membership Requests

The CHERI Alliance welcomes applications from forward-thinking companies looking to shape the future of cybersecurity. Interested companies can apply via the CHERI Alliance website or contact us directly at the email address provided for more details.

The CHERI Alliance has received funding from the Department for Science, Innovation and Technology (DSIT, UK).

###

About The CHERI Alliance

CHERI Alliance is a community interest organization promoting the global adoption of the Capability Hardware Enhanced RISC Instructions (CHERI) security technology across the computing industry. Building on over a decade of pioneering research by the University of Cambridge and SRI International, CHERI introduces a proven architecture designed to enhance system security through fine-grained memory protection and software compartmentalization. The Alliance is actively engaging with industry, academia, and the public sector to standardize and implement CHERI across a diverse range of computing platforms. Founding members include Capabilities Limited, Chevin Technology, Codasip, Critical Technologies, CyNam, DSTL, the FreeBSD Foundation, Google, LMT, lowRISC, National Cyber

Security Centre (NCSC), OpenHW Group, Parvat Infotech, SCI Semiconductor, SRI, Swansea University, TCCoE, TechWorks, the University of Cambridge, the University of Birmingham, and the University of Glasgow. To learn more, visit http://www.cheri-alliance.org

Media Contact

Tora Fridholm

tora.fridholm@cheri-alliance.net

Company Contact:

CHERI Alliance

E. tora.fridholm@cheri-alliance.net
W. https://cheri-alliance.org/

View Online

Additional Assets:

Newsroom: Visit our Newsroom for all the latest stories:
https://www.cheri-alliance.pressat.co.uk