EINPRESSWIRE

SCI Semiconductor announces global-first CHERI enabled devices and Early Access Program

SCI announce global-first CHERI-enabled family of devices, based on the RISC-V RV32E architecture and leveraging the Microsoft CHERIoT-Ibex processor core.

LONDON, UNITED KINGDOM, October 23, 2024 /EINPresswire.com/ -- 22nd October 2024 IoT Security Foundation Conference, IET, London, UK.

SCI Semiconductor are very pleased to announce the global-first CHERI-enabled family of devices, based on the RISC-V RV32E architecture and leveraging the Microsoft CHERIoT-Ibex processor core. Targeting a wide variety of applications, spanning from simple microcontrollers through to advanced embedded applications, this new family of devices will finally deliver CHERI technology as a commercial reality in 2025.

> Over 70% of modern software vulnerabilities are based on memory safety bugs, creating the explosion of cyber-security attacks estimated by McKinsey to create more than $1 Trillion of damage annually.”
>
> *SCI Semiconductor*

Over 70% of modern software vulnerabilities are based on memory safety bugs, creating the explosion of cyber-security attacks that are estimated by McKinsey to create more than $1 Trillion of damage annually. Software reuse is essential to low-cost development but rapidly escalates the scope of attacks, which are endemic in modern code bases globally.

The new ICENI family of microprocessors from SCI Semiconductor leverage industry-leading CHERI architectural extensions, via the Microsoft CHERIoT-Ibex RISC-V core, plus capability-aware high-performance systems and peripherals, to deliver the world’s first high-integrity intrinsically-memory safe devices. The device architecture supports efficient fine-grained hardware enforced compartmentalisation with safe object-granularity sharing built atop the complete spatial and temporal memory-safety guarantees that the hardware enforces. This combination enables fearless code reuse by tightly restraining the blast radium of attacks, even in third-party code and without requiring complete rewrites. Regulations such as EU product liability directives, are easier to comply with when most of the reused code can be removed from the end product’s attack surface.
The family is specifically designed for applications with high-integrity, high-availability, or high-

confidentially requirements, including defence and aerospace, critical infrastructure, industry 4.0, and medical domains, although any application where confidential information, control, or command requirements will welcome this critical protection.

Haydn Povey, Chief Executive, SCI Semiconductor stated, “Following successful demonstration of the ICENI technology earlier this year at CyberUK ’24, we are extremely pleased to announce the availability of this new family of devices that finally delivers on the promise of safe and secure compute. The ICENI family marks the start of a new epoch of secured devices, secured applications, and secured society. The modern cyber-security industry is focused on treating the technological symptoms of poor hardware and software architecture, with CHERI and the new ICENI device family, we can now finally start to treat the disease, enabling rapidly code reuse without importing vulnerabilities, accelerating development and reducing update requirements.”

The ICENI family of devices leverages the open-source CHERIoT Platform a hardware-software co-designed platform that extends the core CHERI guarantees and showcases the possibilities of a pure CHERI system. CHERIoT was originated by Microsoft Research and is now maintained as a cross-vendor open-source project, with Microsoft and SCI Semiconductor as co-owners of the repository, plus contributions from Google and a rapidly evolving host of ecosystem partners including lowRISC, the leader in open-source hardware IP.

David Weston, VP of Enterprise and OS Security at Microsoft added “Microsoft is pleased to see that the open source CHERIoT Ibex core is being used by SCI Semiconductor in an upcoming silicon product. We believe that CHERI is a promising technology that can be used to enhance computer security, and we are happy to see it making its way into production silicon. This is one of the main reasons why Microsoft developed and open sourced the CHERIoT Ibex core.”

SCI are additionally very pleased to announce the ICENI family Early Access Program, which will enable selected customers and partners early access to silicon devices, alongside advanced development systems. These systems leverage the lowRISC Sonata platform enabled by the UKRI Digital Security by Design program. Selected partners can start development immediately on the EAC program with rapid portability to silicon devices in 2025, accelerating to transition to next-generation Memory Safe systems.

For more information on the SCI ICENI family of devices, early access program, applications and technical documentation, please contact info@scisemi.com
About SCI Semiconductors
www.scisemi.com
https://cheirot.org
SCI Semiconductors was formed to lead the commercialisation of CHERI technologies and is a founder member of the CHERI Alliance. With a strong focus on secure and high-integrity computing, the organization has built a team of recognised industry leaders, with decades of leadership in security, processor IP and chip design, and high-integrity software. With multiple

existing projects developed on the prototype Arm Morello test chip, the team focused on enablement of the smaller, simpler, and nimbler, Microsoft CHERIoT Ibex processor.

About CHERI Technology

CHERI, or Capabilities Hardware Enhanced RISC Instructions, has been developed over the last decade by a wide array of leading academic institutions, including University of Cambridge; alongside critical commercial partners, including Microsoft and Arm; and key US & UK governmental stakeholders, including SRI International, DARPA, UKRI and the Department for Science, Innovation and Technology (DSIT).

Targeting the 70% of cyber-attacks that are based on memory misconfiguration and misuse, this revolutionary memory safety technology resolves vast swathes of modern attack vectors, removing the ability to escalate attack points and manipulate computational pointers. Enforcing the dual principals of Least-Privilege and Intentionality, it now becomes possible to define specific high-integrity capabilities and bind software into architecturally protected compartments.

About the CHERI Alliance

https://cheri-alliance.org

CHERI Alliance is spearheading 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 SRI International and the University of Cambridge, CHERI introduces a revolutionary 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. Supported to date by DARPA, UKRI, EPSRC, ERC, Google, Microsoft and Arm, CHERI is a major asset in the fight against cybercrime.

The Digital Security by Design initiative helped promote and create a CHERI ecosystem in the UK. SCI Semiconductor are building on top of this open source bedrock to extend the work beyond initial adoption, and evolve the global ecosystem to make CHERI available commercially, worldwide.

Mr H N Povey
SCI Semiconductor Limited
info@scisemi.com

This press release can be viewed online at: https://www.einpresswire.com/article/753608777