The future of Embedded Security?

SCI Semiconductor delivers CHERI-based security fit for critical infrastructure

THE FUTURE OF EMBEDDED SECURITY?

SCI Semiconductor Delivers World's 1st CHERI-based Microcontrollers

By Haydn Povey, CEO of SCI Semiconductors

Welcome to the Future of Embedded Security

By 2027 is it estimated that the cost of global cybercrime will exceed $23 Tillion USD *(yes, trillion with a "T")* annually, equivalent to China's annual GDP. While this is an astounding number, the bigger surprise is that we largely understand the technical issues that criminals use to impact systems and have done for over 50 years. Many reports, including analysis from Microsoft and Google, acknowledge that 70%+ of Critical Vulnerabilities & Exploits (CVE) are Memory Safety orientated, and these are widely unlisted to gain unauthorized access to systems, to escalate attacks, to steal credentials, and ultimately to hold large critical infrastructure to ransom.

A New Hope

SCI Semiconductor was launched by industry veterans from Arm and Microsoft to adapt CHERI *(Capability Hardware Enhanced RISC Instructions)* technology for a new era of embedded computing. Having traditionally focused on performance and low power, the industry is now seeing a third epoch based around security requirements, to both support legislation and regulation, and critically to embrace the fearless code reuse required to bring down the development costs and reduce the skills shortages impacting the industry.

ICENI™ devices will be released across 2025 and are the first commercial CHERI-enabled devices available globally. The devices will ship with a variety of peripherals and is initially targeted at regulated industries where security and meeting legislative requirements are paramount. Critical infrastructure markets, including smart energy, aerospace, automotive, medical, and industrial applications are targeted due to inherent security regulations and legislation, coupled with a strong requirement to reduce the costs attributed to traditional formal methods. At embedded world, SCI will also highlight the flexible development platforms partners are already utilizing to meet the challenges of Memory Safe computing, resolving confidentiality of systems, plus additionally high integrity and availability requirements.

The "S" to IoT

The traditional joke of "The 'S' in IoT stands for security" is an unfortunate reality. Too many organizations consider security late, or never at all. Often security is perceived as a "necessary evil" rather than fulfilling consumer demand. The EU Cyber Resilience Act and RED legislation are challenging this assumption, but the industry still incorrectly views security as a costly insurance policy, because all code should "just be written correctly." As an industry we know this is impossible, and yet we continue to falsely assume products ship with perfect code and zero flaws.

With the ICENI™ devices, plus underlaying CHERI technology, it is now possible for security to transform into a business benefit, that creates significant value along the supply chain, for developers, integrators, and end users. Benefits can be attributed the five core concepts:

Software Supply Chain Benefits

- Fearless code reuse is enabled through robust fine-grained isolation, significantly lowering software development cycles and accelerating time to market
- Limiting the "blast radius" of any attack, providing a "run-flat tire" for applications
- Maintain system availability by automatically restarting compartments that are compromized

Cost Efficiency Benefits

- Simplified lower-cost development
- Fearless code reuse via simple recompilation; no lengthy code re-writing to support custom TEE's
- > 70% of bugs that would be vulnerabilities on other platforms mitigated, reducing the cost of the upgrade treadmill

Enterprise Mission Critical Benefits

- Enhanced integrity ensures exploits are trapped before data can be corrupted
- Improved availability ensures system stability isn't impacted by compartment crashes
- Fine-granularity compartmentalization supports rapid and reliable restarts after attack detected

Application Security Benefits

- Multi-stage secure boot compartmentalization enables progressively reduced privileges for each stage, minimizing the attack surface, and reducing the costs associated with attacks
- Compartmentalization ensures that a compromised function cannot expose other software to attackers
- CVEs in third-party components are isolated within the system

Legislation & Regulation Benefits

- Delivering standard hardware-enforced framework reduces the cost of legislation
- Reduced application specific security requirements low costs and simplifies solutions
- Simple purchasing requirement ensure organizations meet customer demands

CHERIoT & CHERI
Resolving the Memory Safety Challenge

Memory safety is a property of computer systems that ensures programs only access memory locations they are permitted to, preventing unintended or malicious behaviour.

- **Security:** Majority of critical software vulnerabilities stem from memory safety violations.
- **Reliability:** Memory errors often lead to program crashes or unpredictable behaviour.
- **Maintainability:** Ensuring memory safety makes debugging easier and reduces technical debt.
- **Compliance:** Many industries now require memory-safe programming to meet regulatory standards.

Core Concepts of CHERI

CHERI is an advanced architectural extension designed to enhance memory safety and software security at the hardware level. Developed over more than a decade by the University of Cambridge, in collaboration with SRI International and funded by DARPA, it is now the leading solution for securing computing systems.

At its heart, CHERI introduces *capabilities*, which are hardware-enforced pointers that integrate bounds checking, permissions, and provenance to mitigate common security. This fundamentally changes the way memory management and access control are handled at the processor level.

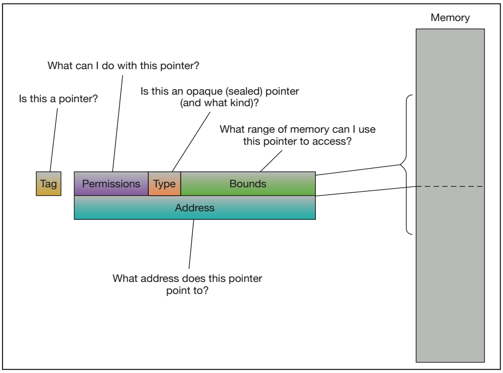
Memory
What can I do with this pointer?
Is this a pointer?
Is this an opaque (sealed) pointer (and what kind)?
What range of memory can I use this pointer to access?
Tag
Permissions
Type
Bounds
Address
What address does this pointer point to?

Figure 1: Traditional Pointers replaced with powerful Capabilities

What are Capabilities?

- **Base and Bounds:** Pointers can only access a designated memory region, preventing buffer overflows.
- **Permissions:** Defines allowed operations (e.g., read, write, execute) to prevent unauthorized memory modifications.
- **Sealing:** Locks capabilities so they cannot be arbitrarily modified, preventing certain types of attacks.
- **Tagging:** Hardware to detect and prevent unauthorized pointer manipulations.
- **Unforgeable**: Capabilities are unforgeable making attacks, such as stack smashing or ROP, significantly harder.

CHERI additionally provides fine-grained memory protection ensuring that every memory access is checked at the hardware level.

The CHERIoT Platform

The CHERIoT platform is a hardware/software co-design project, and the smallest supported implementation of CHERI optimized for small, low- power devices.

Key innovation in CHERIoT include:

- **Secure, Compartmentalize, Real-Time Performance** with low power consumption suitable for a wide array of embedded and IoT applications.
- **Efficient Capability-Bound Memory Protection** for preventing common vulnerabilities such as buffer overflows, use-after-free, and privilege escalation.
- **Hardware-Enforced Software Compartmentalization** to securely isolate different system components, preventing one compromised module from affecting others.
- **Privilege-separated RTOS** with a Trusted Compute Base of only around 300 instructions.
- **Compartmentalization Model** designed for ease of use from higher-level languages.

Feature	Traditional MCUs	ICENI CHERIoT-Based MCUs
Memory Protection	Protect limited number of regions (MPU) or protect pages (MMU)	Object-granularity memory safety for unbounded numbers of objects.
Compartmentalization	Software-based isolation (MPU, TrustZone)	Fine-grained, hardware-enforced compartments
Security Against Buffer Overflows	Software mitigations only	Hardware prevents overflows entirely
Power Consumption	Low power but significant security /power trade-offs for usable MPU regions	Secure execution without sacrificing power efficiency
Use-After-Free Prevention	Traditionally absent	Hardware prevents invalid pointer usage

Table 1: Comparison of ICENI security vs traditional models

Introducing ICENI™
The World's Most Secure MCU

PRODUCT OVERVIEW

ICENI, the world's most secure MCU for securing against memory safety exploits, is a device family of 32-bit highly secure microcontrollers, delivering hardware-enforced memory safety and robust isolation of software at the edge.

ICENI is **secure by design**, eliminating entire classes of vulnerabilities through hardware-enforced memory safety. **It brings simplicity**, being tailored for low-power embedded applications to ensure seamless migration to memory-safe computing. At the same time, **ICENI delivers performance without compromise**, providing real-time responsiveness and deterministic execution.

- ✓ Digital Security by Design
- ✓ 100% Memory Safety
- ✓ Hardware Compartmentalisation
- ✓ Fearless Code Reuse
- ✓ Scalable Device Roadmap

In partnership with

Microsoft Google

KEY FEATURES

Robust Security – Hardware-level CHERI-enabled security against cyber threats.

Advanced Performance – Optimized processing architecture with high throughput and low latency.

Energy Efficiency – Low-power design ensures reduced operational costs and improved sustainability.

Scalability – Modular platform for entry-level to enterprise-scale deployments.

Interoperability – Standards-based design for seamless integration.

Future-Proof Design – Ready for AI, ML, and data-intensive analytics.

Secure. Resilient.
Uncompromising

SCI Semiconductor