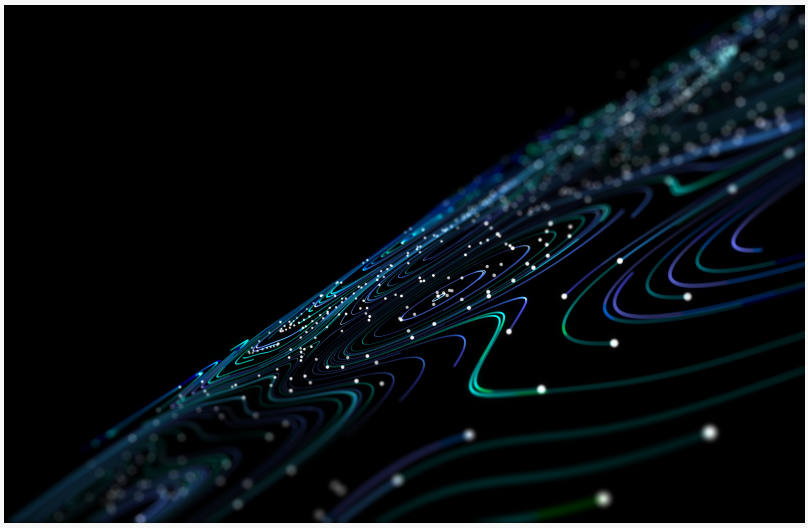
AdaCore Research Proves Novel Solution for 'Security by Default'

BRISTOL, UNITED KINGDOM, June 12, 2024 /EINPresswire.com/ -- In an age of increasing security breaches and cyberattacks, the need for robust and comprehensive security mechanisms within embedded real-time systems is paramount.



AdaCore Research Proves Novel Solution for "Security by Default."

Through its research, AdaCore (https://www.adacore.com/) has demonstrated how combining memory-safe hardware with memory-safe software results in a mutualistic layered approach to security and increases the assurance of embedded real-time systems. More specifically, this research describes the development steps and subsequent evaluation of a security-hardened Ada runtime executing on Arm's Morello CHERI extended ISA microprocessor.

AdaCore is delighted to present this research during ERTS https://erts2024.org/ 11th - 12th June. Paul Butcher, the UK Programme Manager for AdaCore, alongside Daniel King, a bare board expert and cross compiler engineer for AdaCore, as part of a team that also includes Johannes Kliemann, a Product Security Vulnerability Manager for AdaCore, will present their paper: "Security by Default - CHERI ISA Extensions Coupled with a Security-Enhanced Ada Runtime."

"As the UK's National Cyber Security Centre (NCSC) states, 'Secure by Default' is defined as 'technology which has the best security it can without you even knowing it's there or having to turn it on.' This principle served as the guiding philosophy of our research." Paul Butcher

The paper summarizes research and development into a 'Security by Default' approach to real-time embedded systems by leveraging the Arm Morello CHERI ISA extensions and a bare-metal security-enhanced Ada runtime. More specifically, a layered approach to security is described that demonstrates the benefits of memory-safe programming languages executing on memory-safe microprocessors.

"Security by design should be at the forefront of all modern systems development, and factoring security into every phase of the development lifecycle is critical to producing demonstrably safe and secure systems. Our paper presents a Security by Default approach, where fundamental security measures are implemented directly into the hardware and software runtime layer. We argue that our CHERI pure capability GNAT Pro for Morello Ada bare metal runtime executing on the Arm Morello board provides a state-of-the-art cyber security platform upon which developers can implement the highest security assurance applications. Furthermore, our solution captures and propagates CHERI hardware-detected capability faults to Ada exception handlers, allowing for new paradigms in security patterns around cyber-recovery and fail-secure-but-degraded." Paul Butcher

The results and insights presented in this research open additional avenues for strengthening the security of embedded real-time systems, ultimately contributing to safer, more reliable, and more secure technology.

Andrea Bristol
AdaCore
07887997922
email us here
