AdaCore TECH BRIEF

Elevate Security Confidence with Memory Safe Hardware and Software

GNAT PRO FOR CHERI

adacore.com

The Ultimate Security Toolkit

GNAT Pro for CHERI enhances memory safety in modern systems and eradicates many memory-related vulnerabilities. It also provides a complete Ada toolchain to build secure applications executing on Arm Morello, a Capability Hardware Enhanced RISC Instructions (CHERI) CPU. Enhancements to the GNAT Pro GCC and LLVM bare-metal Ada runtimes bring automated CHERI pure-capability memory allocators and other novel security features to the developer, permitting new security-by-design paradigms to systems development.

GNAT Pro for bare metal supports three different runtime libraries: “light”, “light-tasking”, and “embedded”; each library builds on the feature set of the former. GNAT Pro for CHERI supports all three bare-metal libraries on GCC and LLVM compilers and offers a feature-rich configuration set for developers. In addition, GNAT Pro for CHERI on the embedded bare-metal runtime features an enhanced exception handler design that allows CHERI hardware traps to be caught by Ada exception handlers.

- **Multi-layered memory protection**
- **CHERI pure capability memory allocators**
- **Works with both GCC and LLVM**
- **Supported on all three GNAT Pro bare-metal runtimes**
- **Propagation of CHERI hardware traps into Ada software exception handlers**

GNAT Pro for CHERI enhances memory safety in modern systems and eradicates many memory-related vulnerabilities.

What is CHERI?

Capability Hardware Enhanced RISC Instructions (CHERI) is a processor instruction set architecture (ISA) extension developed by the University of Cambridge that provides fine-grained memory protection and compartmentalization at the hardware level. Through a hybrid capability system model, CHERI enforces that software can access memory only according to the bounds and permissions that have been granted to it, thus preventing common memory safety vulnerabilities such as buffer overflows.

The CHERI technology can be applied to bring memory safety to traditionally unsafe languages, such as C or C++, with minimal changes to an existing codebase. CHERI can also be applied to memory safe languages such as Ada and Rust to provide additional memory safety guarantees when using unsafe parts of the language.

About the CHERI Initiative

Digital Security by Design

DSbD is a programme supported by the UK government to transform digital technology and create a more resilient and secure foundation for a safer future. DSbD involves a significant collaboration between academia, industry, and government with an essential emphasis on evaluating the security benefits of Capability Hardware Enhanced RISC Instructions (CHERI).

In partnership with The University of Cambridge and Arm, the initial CHERI initiative has also received funding from the US government through SRI International via the Defense Advanced Research Projects Agency (DARPA, the central research and development organization of the Department of Defense (DOD)).

Using GNAT Pro for CHERI

All industries are looking for viable solutions to the massively disruptive threat of cyber attacks. This requirement often presents itself as mandatory or recognised compliant industry frameworks that describe protocols for preventing and detecting unauthorized electronic interaction. A prime example is Aerospace and Defense, which advocates the usage of guidelines ED-202A/DO-326A, titled “The Airworthiness Security Process.” Another example is ISO/SAE 21434:2021, which defines cybersecurity engineering requirements for road vehicles. Industries, such as space, rail, and nuclear, have equivalent data usages.

High Assurance Security Measures

GNAT Pro for CHERI provides mechanisms that protect against threat conditions and scenarios that could lead to loss of privacy, integrity, or availability of identified security assets. Where an attack vector involves memory safety vulnerabilities like a buffer overflow, the GNAT Pro for CHERI architecture acts as a security measure that will reduce or stop the damage caused by the attack. For example, if the attack intends to expose a security asset within the system, i.e., violate a security requirement regarding asset privacy, GNAT Pro for CHERI’s fine-grain memory protection results in a high-assurance security measure. The attacker may trigger an exploit, but the hardware trap will detect the violation and guard against unauthorized memory reads/writes. The same feature provides a security measure that enforces the security asset’s integrity. By bounding memory accesses, we ensure neighboring data is not overwritten and corrupted.

While the security measure must still detect the event even if the attack only intends to cause disruption or loss of availability, it must also satisfy security requirements that minimize or eradicate the loss of service, for example, recovery, isolation, or damage limitation. GNAT Pro for CHERI’s ability to propagate CHERI capability faults into Ada runtime exception handlers provides detection and countermeasure options to respond to the loss of service attack, acting as an additional high assurance security measure.

For examples of the types of attacks CHERI can guard against, check the AdaCore GitHub site

Advanced Verification Testing

Using GNAT Pro for CHERI, we can isolate security assets in deployed systems and significantly enhance security verification testing by adding sophisticated anomaly detection (detecting memory-related software bugs). To understand why this is important, consider the resultant behavior of a standard (non-CHERI) CPU executing an application that does not use Ada runtime constraint checks. When a triggered software bug results in an out-of-bounds memory read or write instruction, the application might exhibit detectable behavior; for example, a segmentation fault may get signaled. However, it could also go undetected, such that the system continues to operate but also transitions into a state where security can no longer be guaranteed. The combination of an Ada pure-capability runtime executing on a CHERI microprocessor architecture eliminates this possibility. In both cases, the transition into a non-secure state will be visible to the verification suite so that the bug can be identified, logged, and mitigated at a higher level in the security plan or fixed and retested. It is also essential to recognize the symbiosis of the pure-capability Ada runtime and the CHERI hardware capability checks; with the combination, we gain the detection guarantee, resulting in a higher quality verification.

To simplify this approach, engineers can use the QEMU-based technology GNATemulator for Morello to execute tests in a virtualized platform on their host machine or in a cloud-based continuous integration pipeline. In addition, we can elevate security assurance even when the final target hardware is not CHERI-compatible through the cross-compilation of embedded application code with GNAT Pro for CHERI and the execution of tests on GNATemulator for Morello.

Start Using GNAT Pro for CHERI

Contact **AdaCore** if you'd like to learn more about the benefits of GNAT Pro for CHERI and start evaluating the toolchain.

Get started with

GNAT PRO | FOR CHERI

AdaCore

adacore.com

arm Morello Program

Digital Security
by Design