AdaCore | Build Software that Matters

Digital Security by Verification: Fuzz Testing on CHERI

João Azevedo
GNATfuzz Team Lead, AdaCore

HISC 2025
HIGH INTEGRITY SOFTWARE CONFERENCE
NOV 13, 2025

Outline

- What is Digital Security by Design (DSbD) and Digital Security by Verification?
- What is CHERI?
- What is Fuzz Testing?
- Fuzz Testing on CHERI
- Conclusion

Digital Security by Design

- 'Security by Design' is a proactive approach to introduce security measures into systems from the very start, rather than as an add-on
- Secure by Design Problem Book, DSTL, UK MOD, April 2025 - "'Secure by Design' is becoming mandated across UK government for securing crown data and services."
- Cyber Resilience Act, European Union, 2024 - "EU regulation that introduces mandatory cybersecurity requirements for hardware and software products"
- Cybersecurity and Infrastructure Security Agency (CISA), United States federal agency within the Department of Homeland Security (DHS) - "Secure by Design principles prioritize the security of customers as a core business requirement."

Digital Security by Design

- 'Security by Design' is a proactive approach to introduce security measures into systems from the very start, rather than as an add-on
- Secure by Design Problem Book, DSTL, UK MOD, April 2025 – "'Secure by Design' is becoming mandated across UK government for securing crown data and services."
- Cyber Resilience Act, European Union, 2024 – "EU regulation that introduces mandatory cybersecurity requirements for hardware and software products"
- Cybersecurity and Infrastructure Security Agency (CISA), United States federal agency within the Department of Homeland Security (DHS) – "Secure by Design principles prioritize the security of customers as a core business requirement."

Digital Security by Design

- 'Security by Design' is a proactive approach to introduce security measures into systems from the very start, rather than as an add-on
- Secure by Design Problem Book, DSTL, UK MOD, April 2025 - "'Secure by Design' is becoming mandated across UK government for securing crown data and services."
- Cyber Resilience Act, European Union, 2024 - "EU regulation that introduces mandatory cybersecurity requirements for hardware and software products"
- Cybersecurity and Infrastructure Security Agency (CISA), United States federal agency within the Department of Homeland Security (DHS) - "Secure by Design principles prioritize the security of customers as a core business requirement."

Digital Security by Design

- 'Security by Design' is a proactive approach to introduce security measures into systems from the very start, rather than as an add-on
- Secure by Design Problem Book, DSTL, UK MOD, April 2025 - "'Secure by Design' is becoming mandated across UK government for securing crown data and services."
- Cyber Resilience Act, European Union, 2024 - "EU regulation that introduces mandatory cybersecurity requirements for hardware and software products"
- Cybersecurity and Infrastructure Security Agency (CISA), United States federal agency within the Department of Homeland Security (DHS) - "Secure by Design principles prioritize the security of customers as a core business requirement."

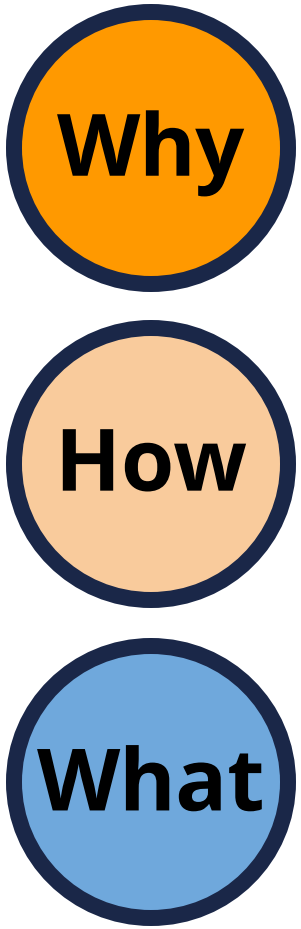
Digital Security by Design

Airworthiness Security Process Specification – ED-202A / DO-326A
Airworthiness Security Methods and Considerations – ED-203A / DO-356A

CHERI – Capability Hardware Enhanced RISC Instructions

- Joint research project of SRI International and the University of Cambridge
- CHERI extends conventional hardware Instruction-Set Architectures with new architectural features to enable fine-grained memory protection and highly scalable software compartmentalization.
- CHERI Alliance – industry initiative spearheading the global adoption of the CHERI security technology across the computing industry

CHERI – Capability Hardware Enhanced RISC Instructions

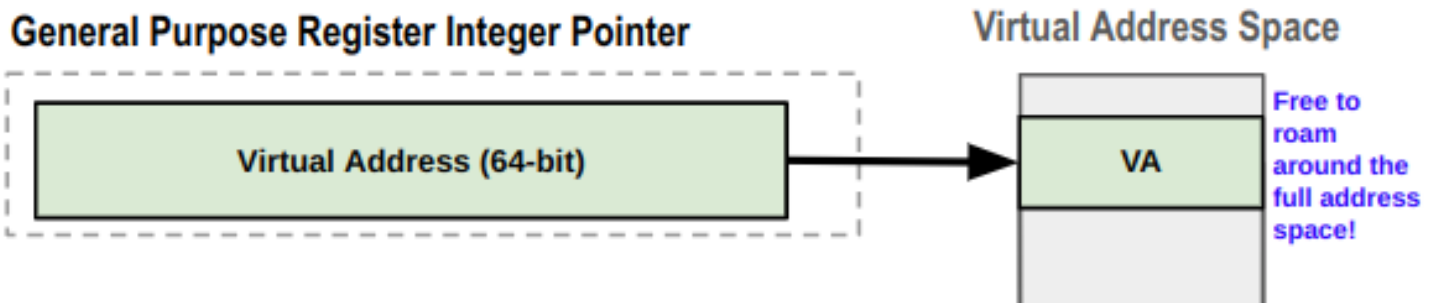


- The current strategy for "handling" cybersecurity is unsustainable (monitor, patch, fix, repeat…).
- Recognition that to be safe, the digital world must secure by default (memory safety is paramount).

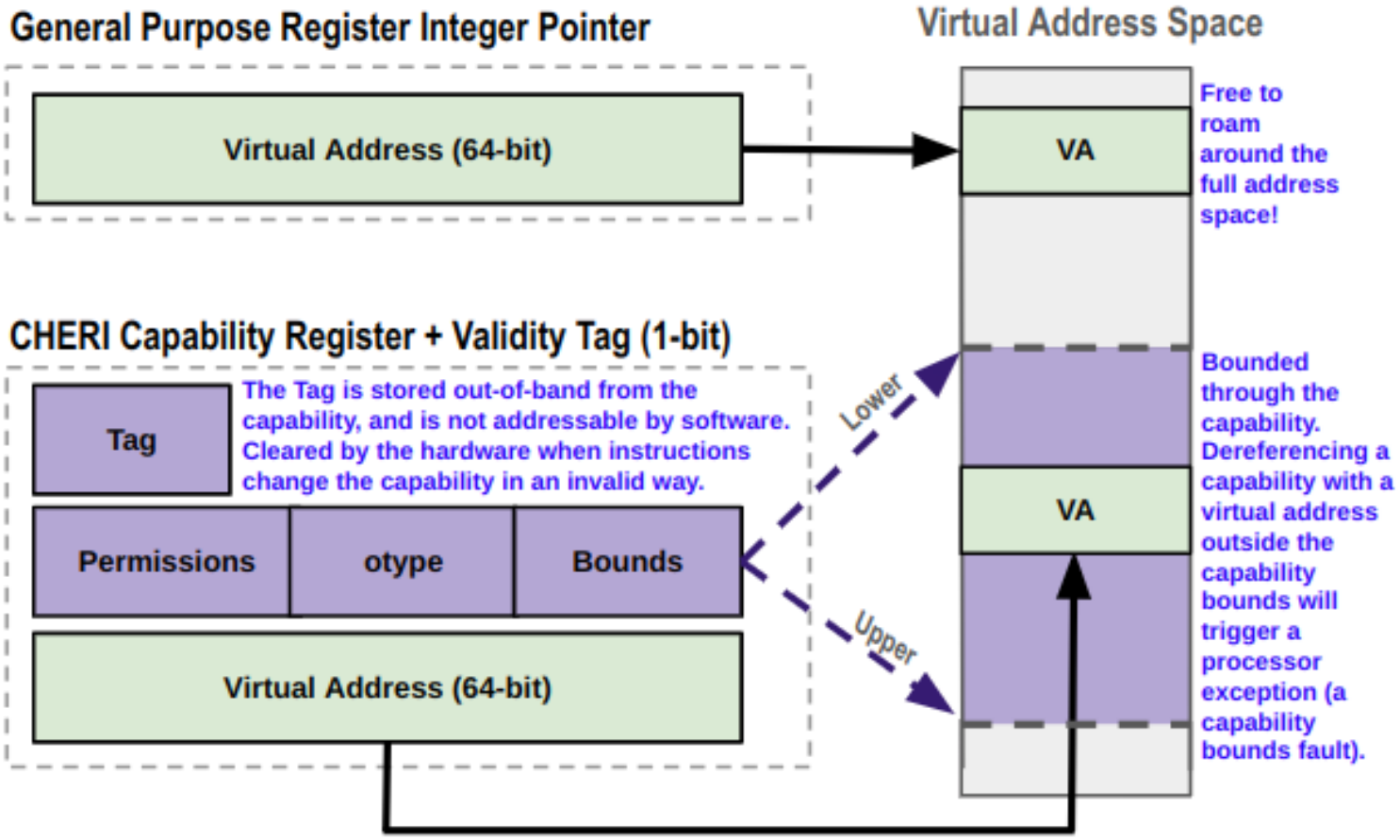
- Adopt a preemptive approach of designing in guards against violation of security properties.

- New CPU architectures guards against violation of security properties (unsafe memory instructions, for example, buffer overflows); upon detection, hardware exceptions are raised.

CHERI – Conventional Pointers



CHERI – Capabilities



Full GNAT Pro Ada Pure Capability runtime for CheriBSD

- Under the Secure Avionics by Design project, funded by the UK RAF Rapid Capabilities Office and overseen by DSTL
- Various Ada Runtimes for the Arm Morello CHERI evaluation board
- CHERI pure capability memory allocators - all memory addresses are CHERI capabilities
- Propagation of CHERI hardware traps into Ada software exception handlers
- Works with both GCC and LLVM

Memory Safe Programming Languages

- Ada
- SPARK
- Rust

Memory Safe Programming Languages

- **Ada** – Unchecked programming
- **SPARK** – Assumptions
- **Rust** – Unsafe programming

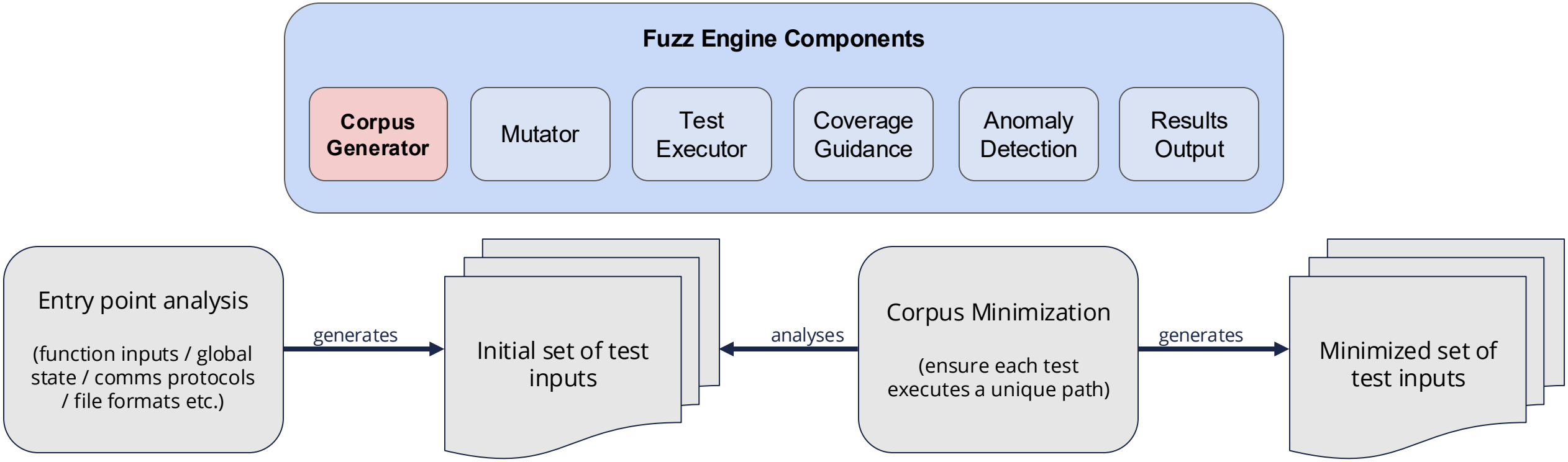
Fuzz Testing

- Automated software testing technique
- Involves the mutation of a corpus of test inputs to create new inputs
- Intermediate tooling includes coverage guidance feedback
- Advanced tooling includes branch solving algorithms (Symbolic execution, redqueen / CMPLOG)

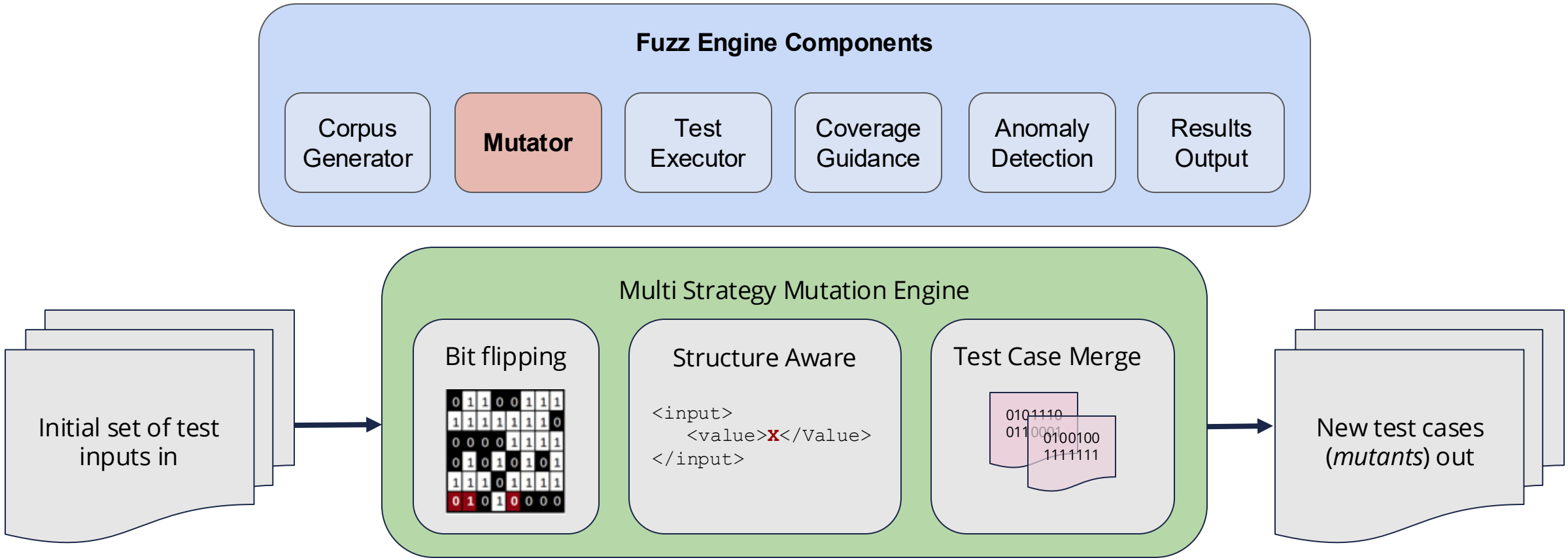
"Program testing can be a very effective way to show the presence of bugs, but it is hopelessly inadequate for showing their absence."

The Humble Programmer, Edsger W. Dijkstra, 1972

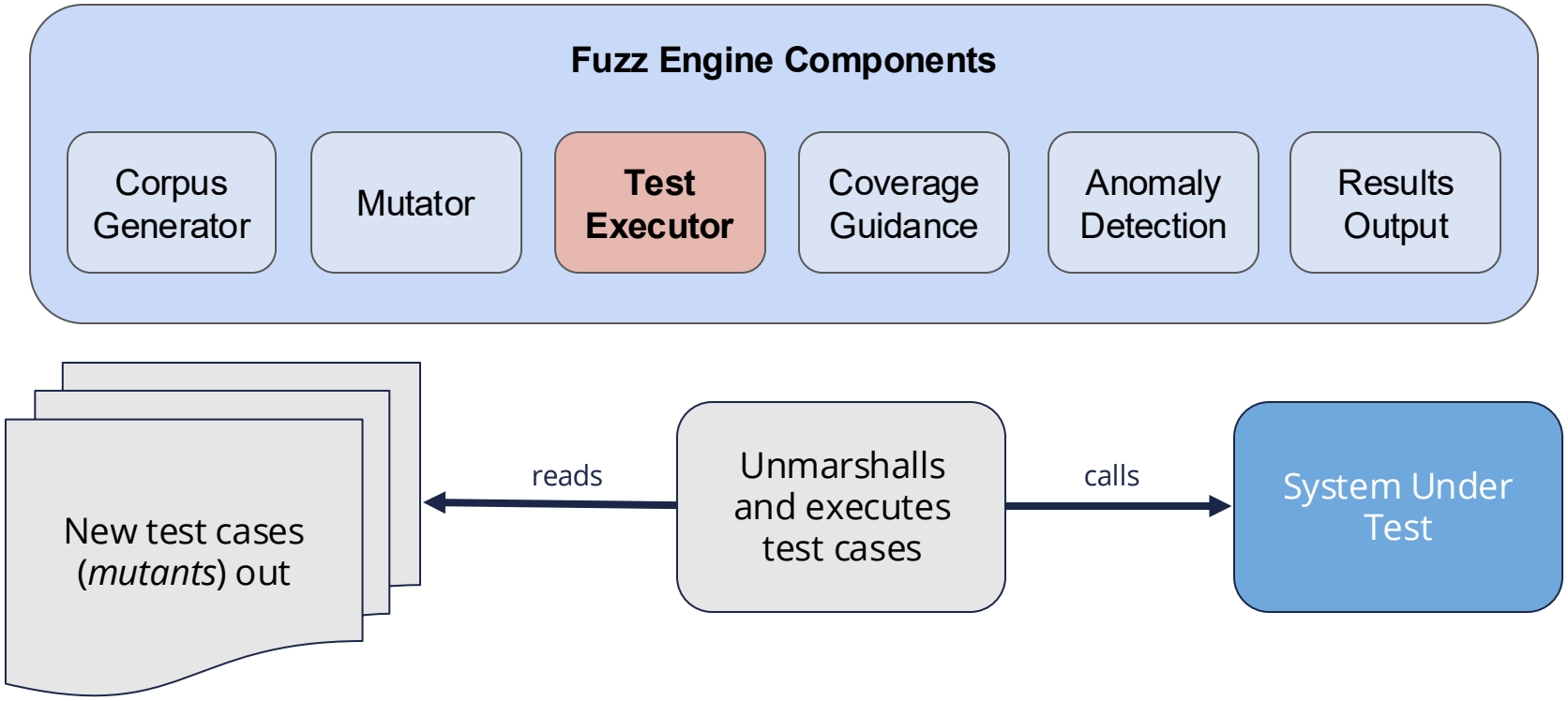
Fuzz Testing



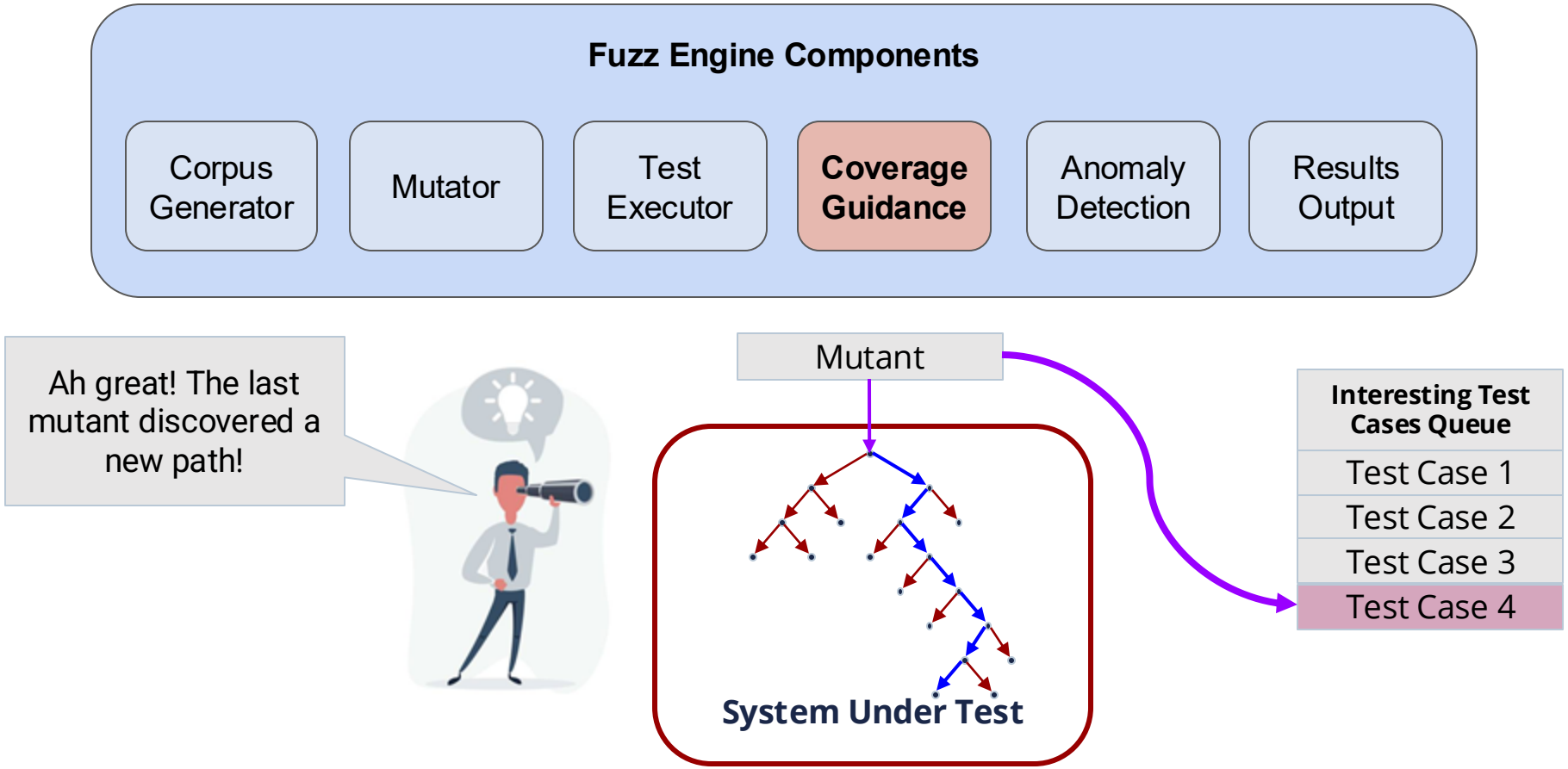
Fuzz Testing



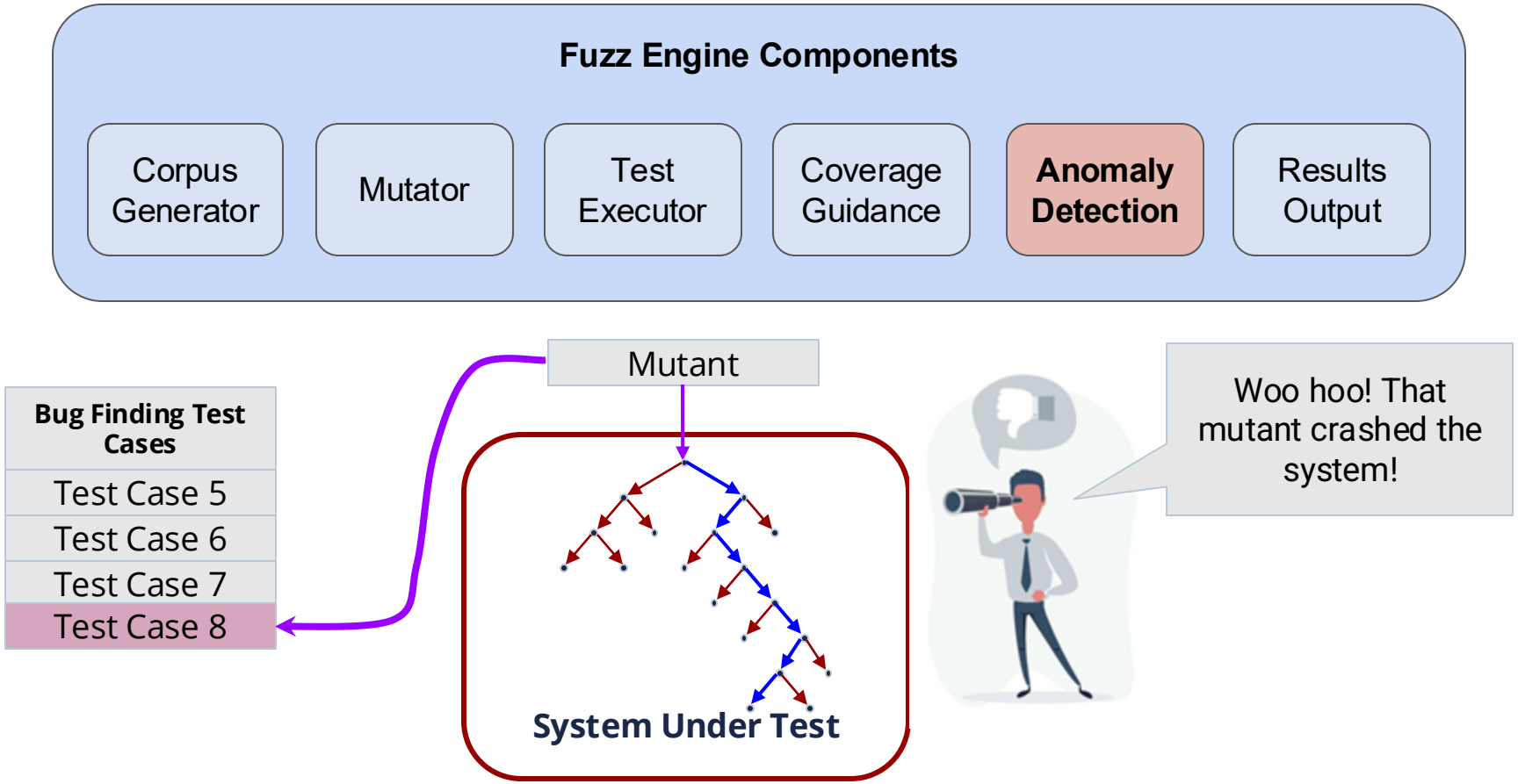
Fuzz Testing



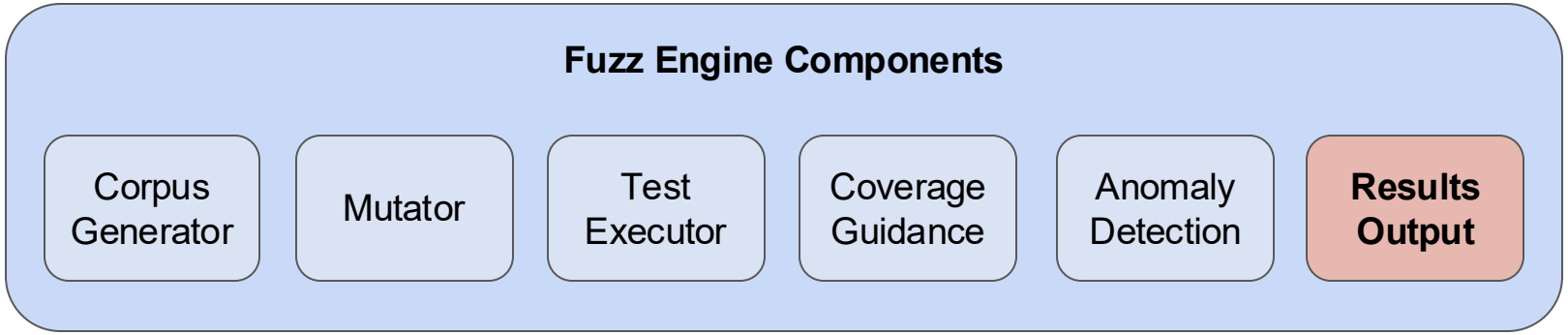
Fuzz Testing

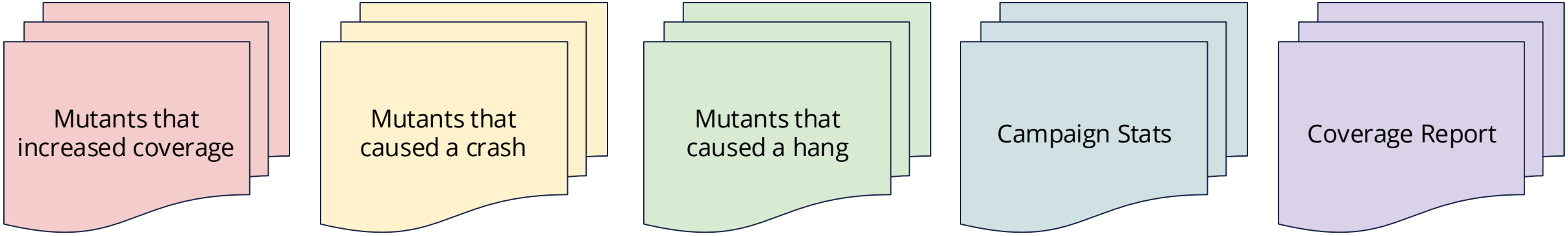


Fuzz Testing

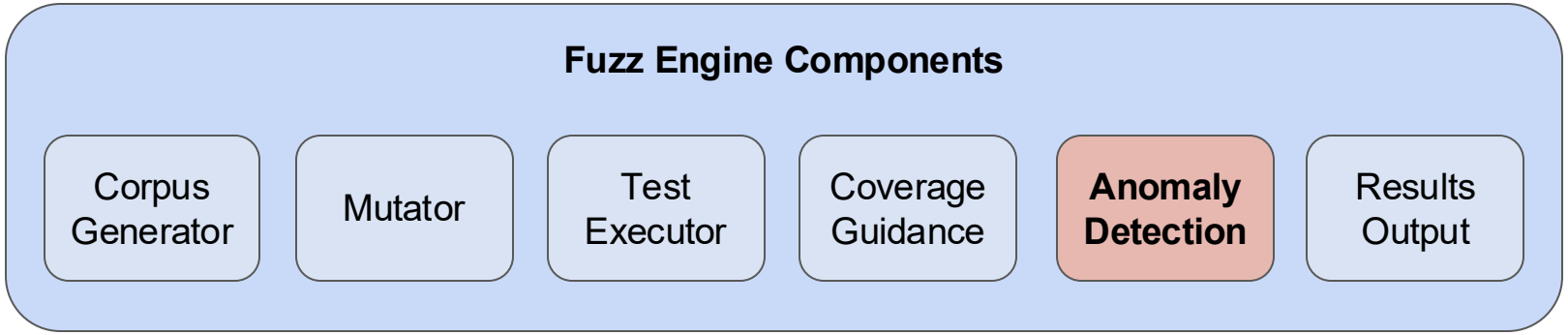


Fuzz Testing





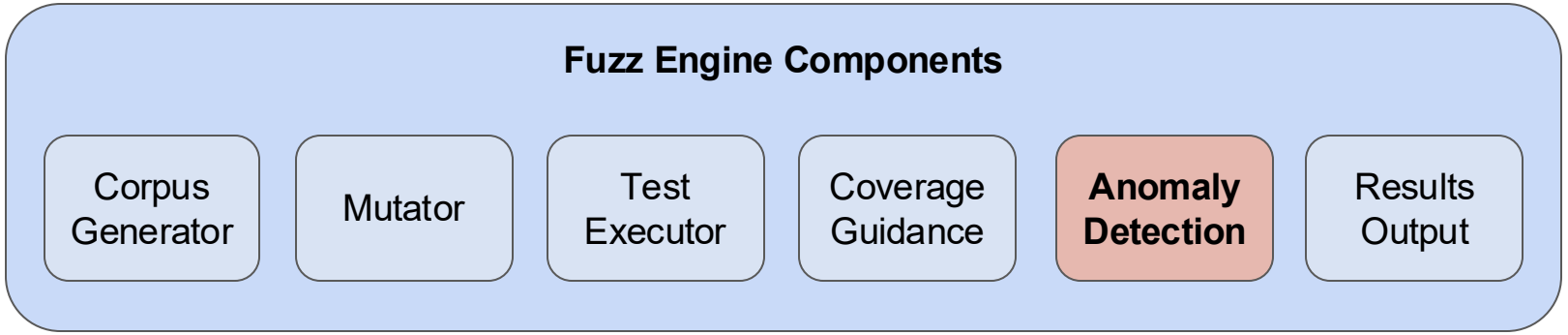
Fuzz Testing



AFL++   LibFuzzer

- Segmentation faults detected through core dump files
- AddressSanitizer or LeakSanitizer

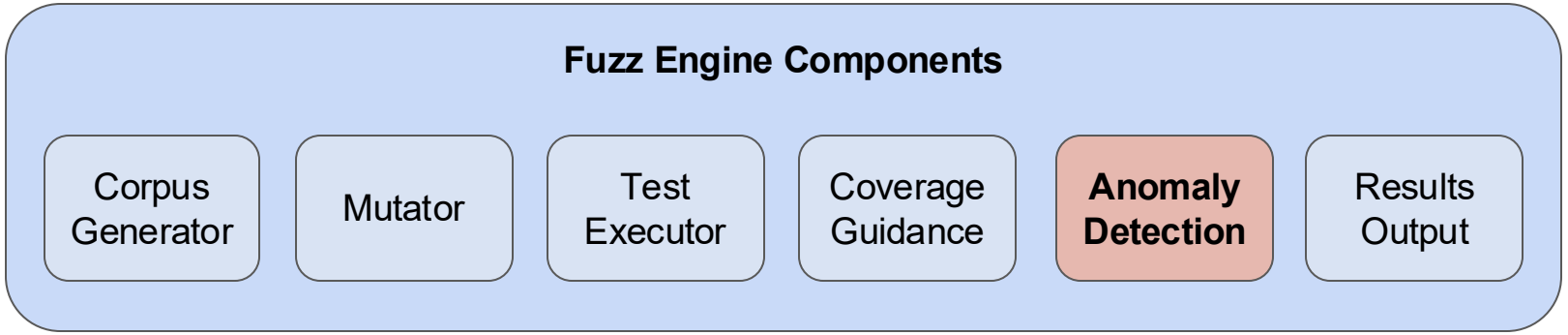
Fuzz Testing



Ada
Run Time Constraint Checks

- Access check / discriminant check / division check / index check / length check / overflow check / range check / tag check / accessibility check / allocation check / elaboration check / storage check

Fuzz Testing on CHERI



Can CHERI help further with anomaly detection?

CHERI Hardware Capability Faults

Fuzz Testing on CHERI

- CHERI is a Dynamic Analysis solution
- Stopping vulnerabilities before they happen is important, but what about high assurance systems where we also want to argue our system is absent of runtime errors before deployment?
- Verification testing on a CHERI architecture is only ever going to be as good as the range of inputs you provide it with (**i.e. not seeing a fault does not mean the fault is not there**)

Fuzz Testing on CHERI – Adaptive Engine

- AdaCore "Adaptive" fuzzing engine
  - Explore the benefits of on-target fuzzing
  - Target CHERI architectures and pure-capability compliant CHERI OS ports
  - Typical smart grey box fuzzer features
    - Corpus generation
    - Mutation engine
    - Coverage-guided feedback via enhancements to GNATcoverage MC/DC coverage
  - Relies on the Full GNAT Pro Ada Pure Capability runtime for CheriBSD
    - Support for bare metal (GNAT Pro Embedded Ada runtime) is a feasible future enhancement

Fuzz Testing on CHERI – Adaptive Engine

- Strengths
  - Portable – only depends on the Ada standard library
  - Catches errors even with unchecked operations
  - It supports every target that GNATfuzz supports
  - Supports fuzzing of C code through bindings from Ada

Fuzz Testing on CHERI – Adaptive Engine

- Current limitations
  - Emulators are too slow to do effective fuzzing
  - No recovery from a timeout
  - It's in-process fuzzing, so if there's memory corruption at some point, the fuzzer could malfunction - CHERI detects these cases

Fuzz Testing on CHERI

	Project sources	Architecture	Duration	Level of Assurance
Continuous Integration	Changes only	Host	X Minutes	Some
Nightly	All	Host	Y Hours	More
Weekly	All	CHERI	Z Days	Lots

Conclusions

- Government entities are increasingly prioritizing 'Secure by Design' principles (and in some regions are already mandated)
- CHERI's enhanced security properties make it an excellent candidate for a memory safe verification environment
- Fuzz testing on a CHERI architecture provides elevated anomaly detection above and beyond the limits of memory-safe programming language runtimes and other dynamic analysis sanitizers

AdaCore | Build Software that Matters

Thank you

João Azevedo
azevedo@adacore.com

HISC 2025
HIGH INTEGRITY SOFTWARE CONFERENCE
NOV 13, 2025