CHERI: Capability Hardware Enhanced RISC Instructions

Hardware-Based Memory Capability Model

CHERI supports Supervisor, user, protected, and system privilege levels. CHERI enforces the security of a targeted memory capability model using the Capability Paradigm. Protection is enforced in software, making it easier to port to different hardware platforms. CHERI's protection is driven by capabilities, which are protected objects with a bit-string that indicates the privilege level of the object. CHERI's protection is also based on physical memory addresses.

Capsicum

Capsicum is an OS-based hybrid capability system for supporting application compartmentalization to mitigate security vulnerabilities. Capsicum shipped in FreeBSD 10, with Google-developed patches providing support for Linux. The main design goal of Capsicum is to make it easy to develop compartmentalized programs. Capsicum isolates tcpdump network processing in a single sandbox, which could allow successful exploits to gain network-access capabilities without having to fully sandbox all TCP/IP applications.

Software Object-Capability Model

Process-based sandboxing on current CPU architectures can be challenging due to the complexity of multidimensional problem space and the number of known and unknown vulnerabilities. CHERI's capability model provides a way to compartmentalize application components, making it easier to develop and deploy secure applications.

Application Programs

Application programs can be compartmentalized in a software object-capability model. This allows developers to identify the complexity of the problem space and the number of known and unknown vulnerabilities. CHERI's capability model provides a way to compartmentalize application components, making it easier to develop and deploy secure applications.

CHERI Processor and ISA Testing and Verification

CHERI allows developers to identify the security benefits and performance costs of object-capability models. CHERI's capability model allows developers to identify the complexity of the problem space and the number of known and unknown vulnerabilities. CHERI's capability model provides a way to compartmentalize application components, making it easier to develop and deploy secure applications.

CHERI Clang/LLVM Support

CHERI's runtime system is built on top of the FreeBSD runtime system. CHERI's runtime system is built on top of the FreeBSD runtime system. CHERI's runtime system is built on top of the FreeBSD runtime system. CHERI's runtime system is built on top of the FreeBSD runtime system.

Hardwared-Assisted, Object-Capability-Based Compartmentalization

Optimum scales up memory processing in a single sandbox, which could allow successful exploits to gain network-access capabilities without having to fully sandbox all TCP/IP applications. CHERI's runtime system allows developers to identify the complexity of the problem space and the number of known and unknown vulnerabilities. CHERI's runtime system provides a way to compartmentalize application components, making it easier to develop and deploy secure applications.

Tesla: Temporally Enhanced Security Logic Assertions

Security properties are often temporal. Will something cause the security to fail before it is detected? Will audit logic eventually detect the exploit? Will an attack cause the security logic to fail before it is detected? CHERI's temporal logic assertions provide a way to verify the security properties of CHERI's runtime system.

Software Object-Capability Model

Process-based sandboxing on current CPU architectures can be challenging due to the complexity of multidimensional problem space and the number of known and unknown vulnerabilities. CHERI's capability model provides a way to compartmentalize application components, making it easier to develop and deploy secure applications.

Application Programs

Application programs can be compartmentalized in a software object-capability model. This allows developers to identify the complexity of the problem space and the number of known and unknown vulnerabilities. CHERI's capability model provides a way to compartmentalize application components, making it easier to develop and deploy secure applications.

CHERI Processor and ISA Testing and Verification

CHERI allows developers to identify the security benefits and performance costs of object-capability models. CHERI's capability model allows developers to identify the complexity of the problem space and the number of known and unknown vulnerabilities. CHERI's capability model provides a way to compartmentalize application components, making it easier to develop and deploy secure applications.

CHERI Clang/LLVM Support

CHERI's runtime system is built on top of the FreeBSD runtime system. CHERI's runtime system is built on top of the FreeBSD runtime system. CHERI's runtime system is built on top of the FreeBSD runtime system. CHERI's runtime system is built on top of the FreeBSD runtime system.

Hardwared-Assisted, Object-Capability-Based Compartmentalization

Optimum scales up memory processing in a single sandbox, which could allow successful exploits to gain network-access capabilities without having to fully sandbox all TCP/IP applications. CHERI's runtime system allows developers to identify the complexity of the problem space and the number of known and unknown vulnerabilities. CHERI's runtime system provides a way to compartmentalize application components, making it easier to develop and deploy secure applications.

Tesla: Temporally Enhanced Security Logic Assertions

Security properties are often temporal. Will something cause the security to fail before it is detected? Will audit logic eventually detect the exploit? Will an attack cause the security logic to fail before it is detected? CHERI's temporal logic assertions provide a way to verify the security properties of CHERI's runtime system.

Software Object-Capability Model

Process-based sandboxing on current CPU architectures can be challenging due to the complexity of multidimensional problem space and the number of known and unknown vulnerabilities. CHERI's capability model provides a way to compartmentalize application components, making it easier to develop and deploy secure applications.