Universität Stuttgart

INSTITUT FÜR
KOMMUNIKATIONSNETZE
UND RECHNERSYSTEME
Prof. Dr.-Ing. Andreas Kirstädter

Master-Arbeit Nr. 1068

Implementierung einer RISC-V Erweiterung in VHDL zur Erkennung manipulierter Sprungziele von indirekten Sprungbefehlen für ein prototypisches Rechnersystem

Methoden
Hardware-Entwicklung

Themengebiete
Rechnerarchitektur

Hintergrund

Die Manipulation der Sprungzieladressen von register-indirekten Sprungbefehlen (engl. Jump Oriented Programming, JOP) ist eine Technik zur Ausnutzung von Sicherheitslücken, durch die ein Angreifer bestimmte Programmfragmente, sogenannte "Gadgets", in nicht vorgesehener Reihenfolge ausführen kann, um beispielsweise an geheime Informationen zu kommen.

Um Schaden durch solche Manipulationen zu verhindern, dürfen register-indirekte Sprungbefehle in vielen modernen Prozessorarchitekturen nur noch speziell dafür vorgesehene Befehle (branch termination instructions) anspringen. Wird ein anderer Befehl angesprungen, löst der Prozessor eine Exception aus. Auch RISC-V spezifiiziert eine entsprechende Erweiterung (Zicflip), die über einen solchen Mechanismus verfügt.

Aufgabenstellung

Die Arbeit gliedert sich in folgende Schritte:

- Einarbeitung in das bestehende prototypische Rechnersystem
- Einarbeitung in die RISC-V ISA und die Zicflip-Erweiterung
- Literaturrecherche zu alternativen Schutzmechanismen gegen JOP
- Implementierung der Erweiterung in VHDL
- Validierung der Funktionalität durch Testprogramme
- Bewertung der Implementierung gegenüber alternativen Schutzmechanismen

Erworbene Kenntnisse und Fähigkeiten

Sie lernen Angriffsszenarien durch die Manipulation von Sprungzielen kennen und erarbeiten sich fundierte Kenntnisse über Konzepte zur Sicherung der "vorwärts gerichteten" Kontrollflussintegrität (engl. forward-edge control flow integrity) moderner Prozessoren. Darüber hinaus lernen Sie mit RISC-V eine moderne und modulare Prozessorarchitektur kennen, deren Erfolg und Verbreitung in Forschung und Industrie ständig zunimmt. Dabei vertiefen Sie Ihre VHDL-Kenntnisse und sind in der Lage, komplexe digitale Systeme zu realisieren.

Voraussetzungen
Rechnerarchitektur und Rechnerorganisation
Entwurf digitaler Systeme

Erwünschte Vorkenntnisse
Programmierkenntnisse in Assembler

Kontakt

M.Sc. Christian Koehler
Raum 1.320 (ETI II), Telefon 685-69001, E-Mail christian.koehler@ikr.uni-stuttgart.de