Universität Stuttgart

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

Master-Arbeit Nr. 1010

Hardware-basierter Schutz der Kontrollflussintegrität in einem RISC-V-Prozessor

Methoden
Entwurf digitaler Systeme
Programmierung

Themengebiete
Prozessorarchitektur
Sicherheit von Rechnersystemen

Hintergrund

Moderne Rechnersysteme implementieren eine Vielzahl von Mechanismen zum Schutz vor Angriffen. Ein solcher Mechanismus basiert auf der strikten Trennung von Daten und Programmcode. Dieser Mechanismus stellt dann zum einen sicher, dass Daten verändert, aber nicht ausgeführt werden können. Zum anderen verhindert er, dass der ausführbare Programmcode verändert werden kann. Dadurch wird einem Angreifer die Möglichkeit genommen, (Schad-)Software einzuschleußen.

Der Angreifer kann den oben beschriebenen Mechanismus jedoch umgehen, indem er den bereits in einem Rechner vorhandenen Code neu verwendet. Dazu muss ihm der Code bekannt sein. Außerdem muss er eine Möglichkeit finden, Rücksprungadressen im Stapel des Rechners zu manipulieren. Er sucht dann Code-Abschnitte, die eine bestimmte Aktion ausführen und durch einen Rücksprung abgeschlossen sind (sogenannte Gadgets). Nun legt er eine Sequenz von Rücksprungadressen auf dem Stapel ab, die jeweils den Beginn eines Gadgets adressieren. Erfolgt ein Rücksprung, leitet dieser den Kontrollfluss auf ein Gadget um. Der Rücksprung am Ende eines Gadgets führt dann zum nächsten Gadget usw. Der Angreifer kann also den Rechner dazu bringen, die Gadgets in einer beliebigen, von ihm durch die Rücksprungadressen definierten Reihenfolge auszuführen.

Aufgabenstellung

Im Rahmen dieser Arbeit soll ein neuartiger hardware-basierter Schutzmechanismus gegen die Manipulation von Rücksprungadressen implementiert werden. Als Basis für die Implementierung dient ein in VHDL beschriebener und auf einem Cyclone V FPGA-Board in Betrieb genommener RISC-V-Prozessor. Der Schutzmechanismus basiert auf der Kapselung von Stapelrahmen in Objekten. Abschließend soll die Funktionsfähigkeit des implementierten Mechanismus durch ausführliche Tests nachgewiesen werden sowie eine Bewertung hinsichtlich seines Hardware- und Laufzeit-Overheads vorgenommen werden.

Erworbene Kenntnisse und Fähigkeiten

Sie setzen sich mit der Sicherheit von Rechnersystemen und einem hardware-basierten Schutzmechanismus auseinander. Durch die Arbeit an einer VHDL-Implementierung eines RISC-V-Prozessors erlernen Sie den Entwurf und die Realisierung von komplexen Hardware-Designs. Mit RISC-V lernen Sie darüber hinaus eine moderne und praxisrelevante Prozessor-Befehlssatzarchitektur kennen.

Voraussetzungen
Entwurf digitaler Systeme
Technische Informatik I
Rechnerarchitektur und Rechnerorganisation

Erwünschte Vorkenntnisse
Programmierkenntnisse in C

Kontakt

M.Sc. Simon Blum
Raum 1.333 (ETI II), Telefon 685-67991, E-Mail simon.blum@ikr.uni-stuttgart.de