CYSEC Cybersecurity TU Darmstadt | System Security Lab | TECHNISCHE UNIVERSITÄT DARMSTADT

Masterthesis – Entwicklung der Hardwarekomponenten einer flexiblen Sicherheitsarchitektur

Hintergrund

Moderne Computersysteme wie mobile Endgeräte, IoT-Geräte oder auch Cloud-Systeme, enthalten Anwendungen von einer Vielzahl an unterschiedlichen Anbietern. Der Bedarf dieser Anwendungen an Systemressourcen (Speicher, Rechenleistung oder auch Zugriffe auf Peripheriegeräte wie Sensoren und Aktuatoren) und das Vertrauen der Endnutzer und Gerätehersteller in diese schwankt von Anwendung zu Anwendung. Viele Anwendungen enthalten sensible Daten der Nutzer oder der Anbieter selbst, die vor unerlaubten Zugriffen geschützt werden müssen. Heutige Sicherheitsarchitekturen bieten jedoch keine ausreichend flexible Separierung von Anwendungen unterschiedlicher Anbieter. Sicherheitslücken einer Anwendung können so häufig die Sicherheit des gesamten Systems gefährden. Ziel ist es daher, eine Sicherheitsarchitektur zu entwickeln, welche es erlaubt, Sicherheitsdomänen für unterschiedliche Anbieter aufzusetzen und diese auf die Bedürfnisse des Anbieters anzupassen. Enthält der Programmcode in einer Domäne eine Schwachstelle, so soll dies nicht die anderen Sicherheitsdomänen gefährden. Die Isolation der Sicherheitsdomänen soll dabei in Hardware durchgesetzt werden und es so erlauben, auch vor starken Angreifern, welche bereits das Betriebssystem kompromittiert haben, zu schützen.

Aufgabe

Im Rahmen dieser Masterthesis sollen Konzepte entwickelt werden, wie die benötigten Isolationsmechanismen, mit möglichst wenig Aufwand und möglichst geringem Einfluss auf die Performanz des Systems, in Hardware realisiert werden können. Im Anschluss sollen die Konzepte auf einer RISC-V Architektur in Simulation umgesetzt und evaluiert werden.

Erforderliche Voraussetzungen

- Erfahrung mit dem Entwurf digitaler Schaltungen
- Erfahrung mit Hardwarebeschreibungssprachen
- Kenntnisse über Busarchitekturen und Protokolle (AMBA)
- Motivation & selbstständiges Arbeiten

Wünschenswerte Voraussetzungen

- IT-Sicherheit Grundwissen
- Kenntnisse über Cache-Architekturen
- Erfahrung mit RISC-V
- Programmierkenntnisse in Scala/Chisel

Kontakt

Bei Interesse an der Masterthesis genügt eine Bewerbung (Lebenslauf, Zeugnisse, aktuelle Leistungsübersicht) via Mail an:
emmanuel.stapf@trust.tu-darmstadt.de

AK Professor Dr.-Ing. Ahmad-Reza Sadeghi
Gebäude S4|14 (CASED Gebäude)
Mornewegstraße 30
64293 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

Februar 2019