

Masterthesis – Entwicklung der Softwarekomponenten 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 flexiblen Sicherheitsdomänen in Software umgesetzt und verwaltet werden können. Die benötigten Isolationsmechanismen in Hardware werden dabei als gegeben angenommen. Im Anschluss sollen die Konzepte auf einem RISC-V Prozessor implementiert und evaluiert werden.

Erforderliche Voraussetzungen

- Programmierkenntnisse in C/C++ und Assembler
- Kenntnisse über Betriebssysteme (memory management, exception handling, I/O, etc.)
- IT-Sicherheit Grundwissen
- Interesse and hardwarenaher Programmierung
- Motivation & selbstständiges Arbeiten

Wünschenswerte Voraussetzungen

- Kenntnisse über den Linux Kernel
- Erfahrung mit RISC-V

Kontakt

Bei Interesse an der Masterthesis genügt eine Bewerbung (Lebenslauf, Zeugnisse, aktuelle Leistungsübersicht) via Mail an:

emmanuel.stapf@trust.tu-darmstadt.de