System Security Lab

TECHNISCHE UNIVERSITÄT DARMSTADT

Abschlussarbeit – Beschleunigung kritischer Softwarekomponenten mit Crypto-Hardware

Hintergrund

Die Vernetzung unserer alltäglichen elektronischen Geräte schreitet immer weiter voran. Schon heute ist das Internet der Dinge oder *Internet of Things* (IoT) allgegenwertig, ob in unseren Wohnungen, Fahrzeugen oder in im öffentlichen Raum. Im Gegenteil, viele dieser Geräte besitzen Sensoren wie Mikrofone, Kameras oder auch biometrische Sensoren, welche bei einer Übernahme des Gerätes massiv die Privatsphäre seiner Verwender gefährden kann. Im industriellen Umfeld (Industrie 4.0) und im Automotive-Bereich, können unzureichende Sicherheitsmaßnahmen sogar lebensgefährlich sein. Ein wichtiger Eckpfeiler zum Schutz kritischer Softwarekomponenten und sensibler Daten ist die konsequente Verschlüsselung der Daten und Kommunikationskanäle mit Hilfe von kryptographischen Methoden. Der Nachteil dieser Methoden liegt in deren verursachten Performance-Einbußen. Eine bessere Performance kann mit spezieller Hardware erreicht werden welche eine schnellere Ausführung von kryptographischen Algorithmen ermöglicht. Doch ist diese Crypto-Hardware kompatibel mit anderen Sicherheitslösungen und kann sie auch von unterschiedlichen kritischen Softwarekomponenten gemeinsam genutzt werden?

Aufgabe

Im Rahmen dieser Abschlussarbeit sollen untersucht werden, welche Lösungen zur Beschleunigung von kryptographischen Algorithmen in eingebetteten Systemen zur Verfügung stehen und ob diese auch kompatibel zu gängigen Sicherheitstechnologien (z.B. ARM TrustZone) sind. Im zweiten Schritt soll ein Konzept erarbeitet werden, wie eine ausgewählte Crypto-Hardware zwischen unterschiedlichen kritischen Softwarekomponenten sicher geteilt werden kann. Im Anschluss soll eine prototypische Implementierung des erstellten Konzepts auf einem ARM-basierten Entwicklungsboard erfolgen.

Erforderliche Voraussetzungen

- C Programmiererfahrung
- Grundkenntnisse Kryptographie
- Motivation & selbstständiges Arbeiten

Wünschenswerte Voraussetzungen

- Erfahrung mit Gerätetreibern
- Kenntnisse der ARM-Architektur

Kontakt

Bei Interesse an einer Abschlussarbeit in diesem Themengebiet genügt eine Bewerbung (Lebenslauf, Zeugnisse, aktuelle Leistungsübersicht) via Mail an:
emmanuel.stapf@trust.tu-darmstadt.de

AK Professor Dr.-Ing. Ahmad-Reza Sadeghi
Gebäude S2|20
Pankratiusstraße 2
64289 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

Juni 2022