Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering
InES Institute of Embedded Systems

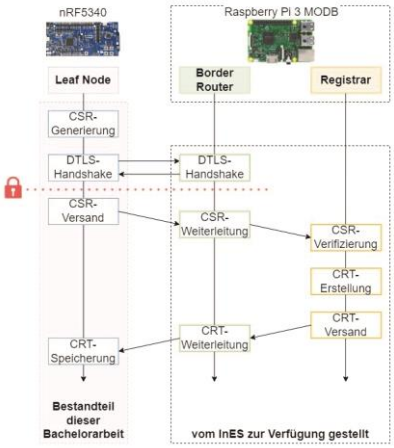
Applying ARM TrustZone for Secure Bootstrapping

Diplomierende
Jan Grau
Yves Wetter

Dozierende
Simon Künzli
Andreas Rüst

Mit der ARM Platform Security Architecture (PSA) existiert ein Framework zur sicheren Implementierung von Applikationen auf Embedded-Geräten. Für CortexM32 / M33 Mikrocontroller kann diese Architektur durch den Einsatz der TrustZone-Technologie implementiert werden. In dieser Arbeit wurde ein Demonstrator entwickelt, welcher die TrustZone-Technologie auf einem nRF5340 mit CortexM33 verwendet. Der Demonstrator bildet den Teilprozess Enrollment over Secure Transport (EST) des Autonomic Secure Bootstrapping Verfahrens ab. Für die Umsetzung wird das Open Source Zephyr-Realtime-Operating-System (RTOS) verwendet, welches mit der Integration von Trusted Firmware-M (TF-M) eine Referenzimplementation für TrustZone bietet. Mithilfe einer Sicherheitsbedürfnis-Analyse des EST-Prozesses werden zwei Umsetzungsvarianten konzipiert, wovon jene mit der direkten Nutzung des PSA-Application Programming Interface (API) für den Demonstrator verwendet wird.

Die Resultate der Arbeit ergeben, dass eine Umsetzung des EST-Prozesses mit der gewählten Umsetzungsvariante für einen nRF5340 basierend auf TrustZone möglich ist. Der Demonstrator beinhaltet eine Zephyr-basierte Implementierung von TF-M. Dadurch wird eine strikte Aufteilung der Applikation in einen sicheren und einen nicht-sicheren Bereich erreicht. Somit ist sichergestellt, dass sicherheitskritische Funktionen und Informationen nur aus dem sicheren Bereich aufgerufen werden können. Neben dem Demonstrator wurden zusätzlich Zeitmessungen für die verwendeten kryptografischen Primitive durchgeführt. Diese Daten werden mit den Zeiten der äquivalenten Umsetzung von Software- und Secure-Elementen verglichen. Die in dieser Arbeit entwickelte Implementation zeigt Performance-Nachteile verglichen mit den meisten herangezogenen Secure Elementen. Die Arbeit zeigt nichtsdestotrotz auf, dass die Möglichkeiten der PSA-Umsetzung mit TrustZone auf dem nRF5340 weitreichend sind und viel Potenzial mit sich bringen. Dies insbesondere, weil für den Einsatz der Technologie keine zusätzliche Peripherie benötigt wird.



Die Abbildung illustriert die einzelnen Schritte des Enrollment over Secure Transport (EST) Prozesses. Der in vorliegender Arbeit entwickelte Demonstrator implementiert die Schritte des Leaf Nodes. Für deren sicherheitskritische Aspekte baut der Demonstrator auf der TrustZone-Technologie auf. Somit wird sichergestellt, dass die sensitiven Operationen des EST-Prozesses gesichert und isoliert vom Rest der Applikation ausgeführt werden können.