Kapitel 9

Sicherheitsansätze

Übersicht

Nach den Grundlagen Grundlagen stellt dieses Kapitel verschiedene Ansätze vor, mit denen die Sicherheit von mobilen und eingebetteten Systeme erhöht werden kann.

Lernziele
Nach Abschluss des Kapitels

- kennen Sie verschiedene Möglichkeiten zur Absicherung von eingebetteten und mobilen Systemen,
- kennen Sie die Vor- und Nachteile der Einzelansätze,
- ist Ihnen die Notwendigkeit von kombinierten Ansätzen bewusst.

9.1 Einleitung

Um die erforderliche Sicherheit in eingebetteten und mobilen Systemen herzustellen, oder das Sicherheitsniveau von existierenden Systemen zu steigern, gibt es eine Vielzahl von möglichen Mechanismen und Ansätzen. Es handelt sich dabei überwiegend um extra für Eingebettete Systeme entwickelte oder angepasste Mechanismen, da Techniken aus der klassischen IT nicht ohne Weiteres angewendet werden können.

Ein möglicher Ansatz ist die Nutzung von Sicherheitsfunktionen der verwendeten Hardware sowie die Implementierung von zusätzlicher Sicherheitshardware. Neben hardwarebasierten Mechanismen kann eine Absicherung von Eingebetteten Systemen auch durch softwarebasierte Ansätze, sowie durch geeignete Kombination beider Möglichkeiten erreicht werden. Welche Sicherheitsansätze einzusetzen sind, ist abhängig vom gegebenen Anwendungsfall und der dadurch geforderten Sicherheit. Ist der Ausfall eines Systems beispielsweise mit hohen Kosten verbunden, muss es stärker abgesichert werden als ein System von untergeordneter Bedeutung.

9.2 Sicherer Bootloader

Ein möglicher Ansatz, um die Sicherheit von eingebetteten und mobilen Systemen zu steigern, ist die Verwendung eines speziell dafür modifizierten sicheren Bootloaders. Als Ausgang dafür kann ein herkömmliches Startprogramm verwendet werden, das mit entsprechenden Sicherheitserweiterungen ausgestattet wird. Wie in Abb. 9.1 dargestellt, wird der Sichere Bootloader vor dem Betriebssystem ausgeführt, wodurch dieses z.B. vor dem Start überprüft werden kann, oder andere Sicherheitsfunktionen angewendet werden können.

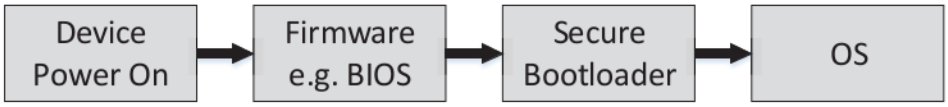

Abbildung 9.1: Bootvorgang mit sicherem Bootloader

Durch die hohe Flexibilität von Software kann ein mit Sicherheitserweiterungen ausgestatteter Bootloader eine Vielzahl von Funktionen und Sicherheitsmechanismen enthalten. Mögliche Beispiele dafür sind:

Da es sich bei diesem Ansatz um eine rein softwarebasierte Sicherheitslösung handelt ist zu beachten, dass die Möglichkeit einer Manipulation des Bootloaders eine erhebliche Schwachstelle darstellt.

Wird zur Steigerung der Sicherheit von eingebetteten und mobilen Systemen ein mit Sicherheitserweiterungen ausgestatteter Bootloader verwendet sind folgende Vor- bzw. Nachteile zu beachten.

9.3 Trusted Platform Module

Ein Trusted Platform Module (TPM) ist ein Hardwaresicherheitschip und eines der Kernelemente von Trusted Computing (TC). Es soll fest mit dem System verbunden sein und bildet dadurch einen hardwarebasierten Vertrauensanker. Der grundlegende Aufbau, sowie die Funktionalität des TPM wird durch die TCG spezifiziert. Da einige Abschnitte der Spezifikation keine konkreten Lösungen zur Umsetzung vorschreiben, sondern eher Empfehlungscharakter haben, sind Abweichungen in den Implementationen verschiedener Hersteller möglich. Zur Kommunikation mit dem TPM stehen verschiedene Schnittstellen zur Verfügung.

Zur Umsetzung des Trusted Computing Konzepts der TCG stellt das TPM drei Kernfunktionalitäten zur Verfügung.

Ab dem Bootvorgang des Systems werden Integritätsmessungen durchgeführt und in speziell dafür vorgesehenen Platform Configuration Registers (PCRs) gespeichert. Man spricht bei diesem Vorgang vom sog. ërweiternëines PCR, da der darin enthaltene Wert nicht ersetzt, sondern mit dem neuen Wert verknüpft wird. Die PCRs spiegeln den aktuellen Zustand des Systems und somit seine Integrität wieder. Dadurch ist es z.B. möglich verschlüsselte Daten an einen bestimmten Systemzustand (an bestimmte PCR-Werte) zu binden.

Diese Funktion beinhaltet einen Generator zum Erzeugen von RSA-Schlüsselpaaren, sowie einen dafür erforderlichen hardwarebasierten Zufallszahlengenerator. Durch die erzeugten Schlüssel ist das TPM in der Lage, sowohl Daten zu signieren und verifizieren, als auch Daten zu verschlüsseln und entschlüsseln. Da die privaten Teile der im TPM erzeugten RSA-Schlüsselpaare den Chip niemals unverschlüsselt verlassen, ist die Verwendung zwingend an das Modul gebunden.

Einer anfragenden dritten Partei kann das TPM den aktuellen Zustand des Systems attestieren. Dazu werden die PCR-Werte und eine in der Anfrage enthaltene Zufallszahl signiert und an die andere Partei gesendet. Durch dieses Verfahren wird nicht nur der Systemzustand übermittelt sondern auch seine Aktualität bestätigt.

Ausgehend von der Spezifikation durch die TCG besitzt ein TPM eine Reihe von diskreten Komponenten. Der Aufbau eines Moduls wird in Abb. 9.2 dargestellt.

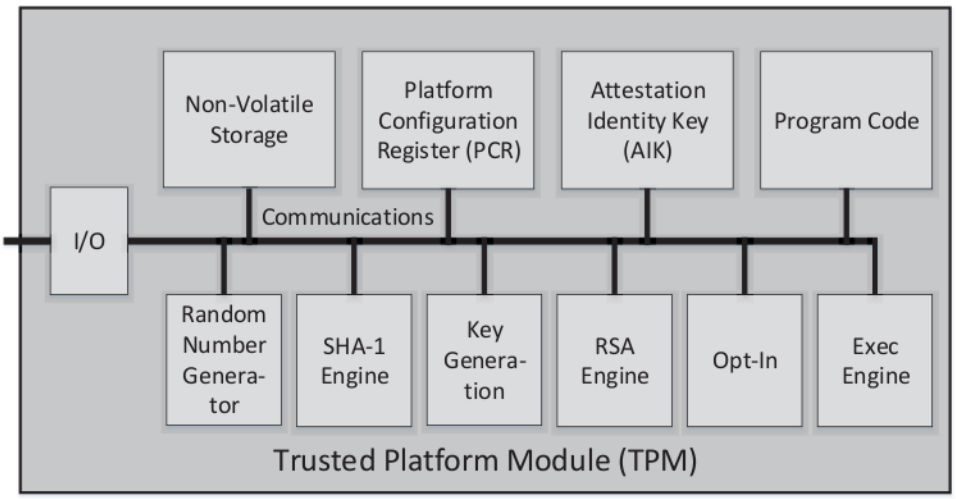

Abbildung 9.2: TPM Blockschaltbild (vgl. [TcgAo14])

Wird zur Steigerung der Sicherheit von eingebetteten und mobilen Systemen ein TPM verwendet sind folgende Vor- bzw. Nachteile zu beachten.

9.4 ARM TrustZone

Bei ARM TrustZone handelt es sich um eine systemische Sicherheitslösung von ARM Limited für eine Vielzahl an Anwendungen. Ähnlich wie beim Ansatz der TCG wird hier eine Trusted Computing Platform aufgebaut, die eine Trusted Execution Environment (TEE) unterstützt. Als TEE wird eine sichere bzw. vertrauenswürdige Laufzeitumgebung für Software bezeichnet.

Als hardwarebasierte Sicherheit ist die TrustZone-Technologie direkt in die entsprechenden Prozessoren (vgl. Tab. 9.1) integriert. Über die Advanced Microcontroller Bus Architecture (AMBA) von ARM wird die Sicherheit auf das gesamte System ausgedehnt. Auch Peripheriekomponenten können durch diese Technologie abgesichert werden.

Neben den Prozessoren werden zusätzlich mit der TrustZone Hardware Library IPs zur Verfügung gestellt, die für den Einsatz der TrustZone-Technologie erforderlich sind.

ARM Cortex-A57	ARM Cortex-A8
ARM Cortex-A53	ARM Cortex-A7
ARM Cortex-A15	ARM Cortex-A5
ARM Cortex-A12	ARM1176
ARM Cortex-A9	

Tabelle 9.1: ARM-Prozessoren mit TrustZone

Die Sicherheit dieser Technologie wird durch folgende drei Elemente erreicht:

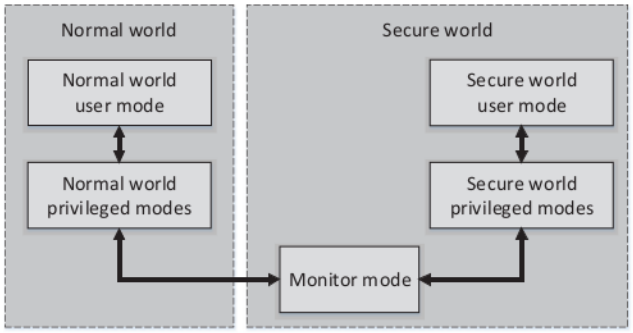

Abbildung 9.3: TrustZone Modes (vgl. [TZ WhitePaper])

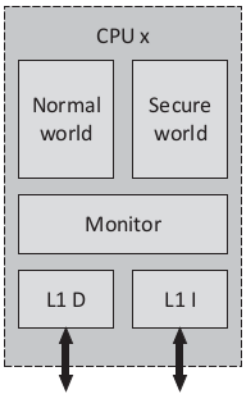

Abbildung 9.4: TrustZone Prozessor (vgl. [TZ WhitePaper])

Wird zur Steigerung der Sicherheit von eingebetteten und mobilen Systemen die ARM TrustZone verwendet sind folgende Vor- bzw. Nachteile zu beachten.

9.5 Freescale High Assurance Boot

Der High Assurance Boot (HAB) ist eine Technologie von Freescale Semiconductor Inc. (kurz Freescale) zur Steigerung der Sicherheit von Eingebetteten Systemen. Sie ermöglicht einen sicheren Bootvorgang (Secure Boot). Durch entsprechende Firmware und einem zusätzlichen OTP (One-Time-Programmable) Speicher ist der HAB direkt in bestimmte ARM-Prozessoren von Freescale integriert. Ist diese Funktion aktiviert führt der Prozessor nur noch korrekt signierten Code aus. Dadurch kann der verwendete Bootloader nicht mehr manipuliert werden und wird deshalb als vertrauenswürdig angesehen. Er bildet somit den Anfang einer Vertrauenskette, an deren Ende z.B. ein sicheres Betriebssystem stehen kann.

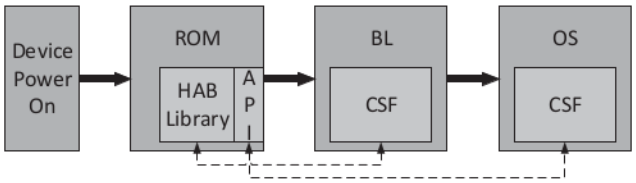

Abbildung 9.5: HAB Bootvorgang (vgl. [FsHabCstUG)]

Wird zur Steigerung der Sicherheit von eingebetteten und mobilen Systemen der Freescale HAB verwendet sind folgende Vor- bzw. Nachteile zu beachten.

9.6 Kombinierte Ansätze

Viele Ansätze zur Steigerung der Sicherheit von eingebetteten und mobilen Systemen weisen erhebliche Nachteile auf, gewährleisten nicht die geforderte Sicherheit oder können einzeln nicht angewendet werden. Anhand der aufgezählten Nachteile der einzelnen Sicherheitslösungen wird dies deutlich.

Durch geeignete Kombinationen lassen sich einige der beschriebenen Schwachstellen ausgleichen, wodurch die Sicherheit des Systems erhöht wird. Um Eingebettete Systeme abzusichern, ist aus diesem Grund der Einsatz von kombinierten Sicherheitslösungen sinnvoll.

Ein Beispiel für einen kombinierten Sicherheitsansatz ist die Kombination: HAB, sicherer Bootloader und TPM.

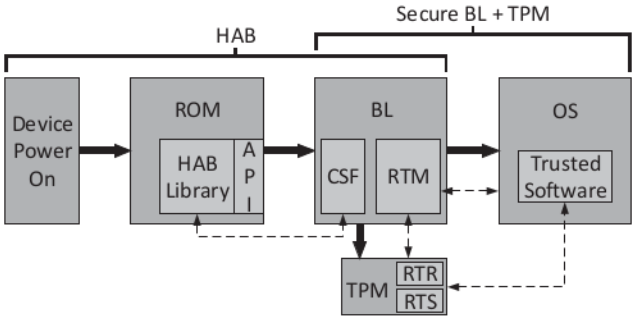

Abbildung 9.6: HAB-BL-TPM Bootvorgang

Wird zur Steigerung der Sicherheit von eingebetteten und mobilen Systemen die Kombination aus einem sicheren Bootloader, dem Freescale HAB und einem TPM verwendet sind folgende Vor- bzw. Nachteile zu beachten.