MASTER OF SCIENCE IN ENGINEERING

Forschungsprojektarbeit des Profils Information and Cyber Security

Sichere Hardwareplattform für IoT-Devices auf ESP32-Basis

Ausgangslage

Im Umfeld von IoT sind sichere Updates oder vertrauenswürdige Plattformen nicht wirklich in Verwendung. Neu gibt es aber Systeme, wie die dritte Generation der ESP32-Bausteine, die Features, wie eFuses Flash Encryption oder Secure Boot unterstützen. Fertige sichere Plattformen, die eine Absicherung erlauben gibt es aber noch nicht.

eFuses erlauben es, Speicherbereiche einmalig zu schreiben und sie anschliessend gegen überschreiben zu sichern. Das ist für den ganzen Speicher sinnlos, kann aber eingesetzt werden, um einen minimalen Bootloader zu schützen. Von da an arbeitet man typischerweise mit Secure Boot, womit einzelne Speicherbereiche vor dem Ausführen auf gültige Signaturen geprüft werden können.

Die Flash Encryption erlaubt es, den Speicher so zu verwenden, dass bei einem Entfernen aus dem System die Daten wertlos werden.

Zielsetzung / Methodik / Vorgehen

Dieses Projekt befasst sich intensiv mit den Absicherungsmöglichkeiten der ESP32-Plattform. In einem ersten Schritt soll ein Proof-of-Concept (PoC) für eine generische Plattform erstellt werden, die es erlaubt, mit Hilfe der bereits vorhandenen Features in der ESP32-S3-Plattform ein System abzusichern. Es soll verhindert werden, dass nicht vertrauenswürdiger Code auf die Plattform gelangt oder dort ausgeführt wird. In mehreren Schritten soll das Konzept verfeinert werden und gegebenenfalls auch um ein TPM-Modul erweitert werden.

In einer ersten Phase sollen Secure Boot und eFuses statisch verwendet werden. In einer zweiten Phase soll geprüft werden, ob das Konzept mit Remote oder Over-the-Air-Upgrades (OtA) ergänzt werden kann und welche Angriffsmöglichkeiten sich daraus ergeben. In der letzten Phase soll geprüft werden, inwiefern der Einsatz von Canaries und ähnlichen Compilertechnologien die Sicherheit weiter erhöht werden kann.

Verlangte Skills: Analytische Ingenieurfähigkeiten, Freude an Hardwarenaher Programmierung in C oder C++

Teilaufgaben

Das Projekt kann in 2 bis 3 Stufen durchgeführt werden: Fortlaufende Projekte 7 (Implementierung eines ersten PoC-Bootloaders mit Secure Boot Absicherung), 8 (Sauberer zwei Phasen Aufbau und Erweiterung mit OtA Upgrades) und 9 (Analyse der Lösung und Demonstration der verbleibenden Angriffsmöglichkeiten, sowie deren Abwehr)

Studienart: [X] Vollzeitstudium
[ ] Teilzeitstudium 50% mit Assistenzanstellung

Projektorganisation: Arbeit in einem Projektteam / Einzelarbeit

Projektfinanzierung: keine

Arbeitsort: Windisch

Advisor: Martin Gwerder