As IoT adoption grows, so does the security risk. Small embedded devices often have limited or software-managed security requiring specialist developers. The launch of the ARM®v8-M Architecture with hardware integrated protection means security is now much easier to implement on these devices. Together with the CMSIS standard, ARM offers a foundation for developers to create secure, scalable solutions for device integrity, asset protection, and communications security.

ARMv8-M Architecture

Launched in November 2015, the ARMv8-M architecture extends ARM TrustZone® technology to microcontrollers. This creates a foundation in hardware that offers security, scalability, and improved debug for small embedded devices and IoT applications.

TrustZone for ARMv8-M is a ground-up architecture specifically designed for resource constrained devices. By creating separate trusted and non-trusted states across the processor system, it significantly limits the hardware and software attack surface. By putting the foundation for security into the heart of the architecture, ARMv8-M ensures security transitions can occur with almost zero overhead and that microcontrollers can continue to offer deterministic interrupt responses.

ARMv8-M enables scalability and secure development for the most energy-efficient to the highest performing microcontrollers; creating new opportunities for traditional embedded and emerging IoT applications.

ARM TrustZone

ARM TrustZone technology is a System on Chip (SoC) and CPU system-wide approach to security that is used on billions of chips to protect valuable services and devices in a diverse range of end markets, including smartphones, tablets, personal computers, wearables and enterprise systems.

TrustZone is hardware based security built into SoCs by semiconductor chip designers who want to provide secure end points and roots of trust. TrustZone technology can be integrated into any ARM based system, from the smallest microcontrollers to high performance applications processors.

Mit der Zunahme von IoT Applikationen wächst auch das Sicherheitsrisiko. Kleine Embedded-Systeme haben meist nur limitierten Software-Schutz, der nur von Spezialisten verstanden wird. Die ARM®v8-M Architektur implementiert Sicherheit bereits in der Hardware und ist dadurch einfach zu handhaben. Zusammen mit dem CMSIS Standard bietet ARM damit die Grundlage für die Entwicklung von skalierbaren Applikationen, die Schutz vor Angriffen integrieren und sichere Kommunikation erlauben.

ARMv8-M Architektur

Im November 2015 wurde die ARMv8-M Architektur mit TrustZone® Technologie für Mikrocontroller vorgestellt. Diese Kombination bildet die Hardware-Grundlage für Sicherheit, Skalierbarkeit und besseres Debugging bei kleinen Embedded Systemen und IoT Applikationen.

TrustZone für ARMv8-M wurde speziell für ressourcenbeschränkte Geräte von Grund auf neu entwickelt. Separate "secure" und "non-secure" Ausführungsbereiche, die das gesamte Prozessorsystem abdecken, reduzieren erheblich die Angriffsmöglichkeiten für Software- und Hardware-Attacken. Die Integration von TrustZone in das Herz der ARMv8-M Architektur erlaubt den Wechsel des Ausführungsbereichs nahezu ohne Overhead, und bietet damit weiterhin deterministisches Interrupt-Verhalten für Mikrocontroller.

ARMv8-M bietet diese Sicherheit sowohl für sehr energieeffiziente als auch extrem leistungsstarke Mikrocontroller und ermöglicht damit neue Embedded und IoT Applikationen.

ARM TrustZone

Die ARM TrustZone-Technologie ist ein Sicherheitsansatz im gesamten System-on-Chip (SoC), der bereits heute in vielen Halbleitern integiert ist, um Dienste und Geräte zu schützen. Die Anwendungen reichen von Smartphones, Tablets und Wearables bis zu Netzwerk-Infrastruktur.

TrustZone implementiert Sicherheit in der Hardware der Prozessor-Systeme und erlaubt damit vertrauenswürdige Endpunkte. Mit ARMv8-M kann die Trustzone-Technologie jetzt auch in kleinste Mikrocontroller integriert werden.