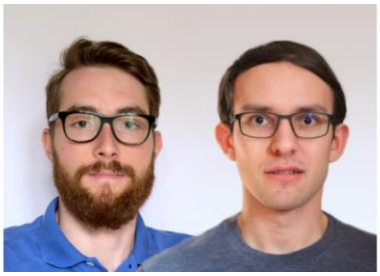
Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering
InES Institute of Embedded Systems

# Secure Boot für System on Chip



Diplomierende
Thierry Delafontaine
Tobias Vögeli

Dozierende
Matthias Rosenthal
Andreas Rüst

Bei vielen embedded Geräten fehlt die nötige Sicherheit vor möglichen Hackerangriffen. Die Hersteller erkennen jedoch langsam die Notwendigkeit, ihre Produkte sicherer zu machen. Die Firma Enclustra wünscht sich mit einem Referenzdesign, ihren Kunden beim Entwickeln eines sicheren Produktes zu helfen. Angelehnt an das Platform Security Architecture (PSA) Framework von ARM wurden drei von Enclustra definierte Anwendungsfälle analysiert. Um diese Anwendungsfälle zu implementieren, wurden verschiedene Sicherheitsfunktionen vom Xilinx Zynq Ultrascale+ MPSoC untersucht und implementiert.

Das Ergebnis ist ein modulares Referenzdesign, welches je nach individuellem Anwendungsfall mit verschiedenen Sicherheitsfunktionen ergänzt werden kann. Die Basis ist ein PetaLinux-Projekt, um den Zynq Ultrascale+ mit einem verschlüsselten und authentifizierten Image zu booten. Es verwendet die Kryptographie-Hardware und Schlüsselverwaltung von Xilinx. Zusätzlich zum Basisprojekt können Funktionen wie Multiboot oder die Tamper-Monitoring-Unit als Module zum Referenzdesign hinzugefügt werden. Die Linux Crypto-API wurde integriert, um die Kryptographie-Hardware des Zynq Ultrascale+ auch unter Linux auf dem FPGA zu verwenden. Dabei wurden Code-Beispiele für verschiedene Algorithmen erstellt, die die Implementierung der Linux Crypto-API vereinfachen. Um kritische Anwendungen zu isolieren, setzt ARM das TrustZone-Konzept in ihren Prozessorarchitekturen ein. Dieses Konzept wurde untersucht und auf dem Xilinx-Evaluierungskit ZCU102 mit OP-TEE als Secure-OS umgesetzt. Dies ermöglicht es einem Benutzer, kritische Anwendungen oder Daten vollständig zu isolieren und zu schützen, selbst wenn Teile des Systems kompromittiert werden.

Schliesslich zeigt diese Arbeit, dass der Zynq Ultrascale+ für eine sichere Produktentwicklung gebaut ist. Es werden nicht nur kryptographische Möglichkeiten, sondern auch Tools für die Wartbarkeit, Zuverlässigkeit und sichere Code-Ausführung angeboten. Das Referenzdesign ist eine solide Grundlage zur Verwendung all dieser Features.

Verwendete Hardware: Mercury XU5 auf einem Mercury+ PE1 Board von Enclustra

Der Zynq Ultrascale+ von Xilinx ist ein SoC (System on Chip) mit programmierbarer Logik und mehreren Prozessoren auf einem Chip.