Bachelor Thesis – Themenvorschlag

OP-Tee mit OpenWRT

Die OP-Tee Spezifikation definiert eine sichere Zone (Trusted Execution Environment) als Companion zum Linux Kernel innerhalb von Geräten. Dies wird normalerweise mit Hilfe der ARM TrustZone Technologie umgesetzt. In dieser sicheren Umgebung können eigene Prozesse ausgeführt werden deren Daten auch vor dem Betriebssystemzugriff gesichert sind. Die Zone eignet sich z.B. um besonders sensible Prozesse zu beherbergen wie z.B. das Ablegen von Private-Keys und das Durchführen von Krypto-Operationen. Auch die CPUs der ads-tec Firewall besitzen verschiedene ARM Prozessoren welche dies unterstützen.
Die Software für die ads-tec Firewalls und Router der IRF-Serie werden bei ads-tec mit Hilfe des OpenWRT Buildsystem compiliert. Das OpenWRT Build System hat jedoch keine Integration für Op-Tee Software Komponenten.

Die ads-tec IRF3 besitzt einen NXP LS1046A Quad Core ARM64 Prozessor mit ARM Trust Zone Integration

OP-TEE
.org

Im Rahmen der Arbeit soll versucht werden prototypisch die ads-tec OpenWRT BuildChain für U-Boot Bootloader und Linux Betriebssystem zu erweitern. Ziel wäre es letztendlich den NXP Op-Tee Testcode (imx-optee-test) zu compilieren und auf der IRF Plattform auszuführen.
Die dafür nötigen Änderungen und Erweiterungen können aus den anderen OpenSource Linux Umgebungen und der Dokumentation von NXP entnommen werden und sollen um Rahmen der Arbeit untersucht und aufgezeigt werden.

Interesse? Oder Alternatividee?
Kontakt: s.pfendtner@ads-tec.de

adstec Engineering