



Maximaler Schutz für Embedded Systeme

„Security“ bezieht sich auf die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität von funktionssicheren Systemen. Bei vernetzten Systemen sind auch die Schutzziele Authentizität und Autorisierung von besonderer Bedeutung.

Mixed Mode kann im Bereich Security bereits langjährige Erfahrung in Kundenprojekten vorweisen. Um das Thema IT- und Cyber-Sicherheit weiter voran zu treiben, engagiert sich Mixed Mode aktiv in Verbänden wie dem Sicherheitsnetzwerk München.

Zudem wurden bei Mixed Mode mehrere Forschungsprojekte wie CONNECT, SecFutur und SIBASE zu dem Thema erfolgreich durchgeführt.

Weitere Informationen

» [Projektüberblick](#)

Projektbeispiele Security

Automotive HSM Firmware mit Anbindung an den AUTOSAR Crypto-Stack für Telematikplattform (E-Call)

- Crypto-Services wie z.B. MAC-Erzeugung, Verschlüsselung und Signatur
- Secure Boot und Secure Storage
- Seamless Secure HSM Update
- Lifecycle-Management (Debug Protection) & Test

Security Konzept und Umsetzung für Industrie 4.0

- Security System-Assessment für Großküchenmaschinen
- Infrastruktur, Key-management und Automatisierung von Signaturen
- Datenverschlüsselung, Code-Signing, HSM-Verwaltung
- Secure-Update und Secure-Boot

Sichere Zugangssysteme in Automotive und Facility mit BLE

- Entwicklung von SDKs für Hardware OEM Produkte mit Fokus auf hohe Sicherheit (Security), Performanz und Energieeffizienz
- Technische Beratung und Konzepterstellung
- Agile Development, Integration und Continuous Integration

Security Toolentwicklungen

- Objektorientierte Applikationssoftware-Entwicklungen für Security-Anwendungen inklusive Kryptokomponenten
- Darunter schnelle Simulatoren und Emulatoren für Chipcard Processor Cores und die angeschlossene Peripherie

Secure Application

Sichere Kommunikationslösung auf Basis von Android Smartphones

SecRec (Secure Reconfiguration)

- ▮ Erforschung der Verbesserung der FPGA-Sicherheit gegen Angriffe durch lokale und partielle Rekonfigurationstechniken
- ▮ Entwicklung eines automatisierten Build-Workflows für die Generierung der partiellen Lösungen
- ▮ Entwicklung jeweils eines Demonstrators für Seitenkanalangriffe sowie Fehlerinjektionsangriffe

SecForCars(Security For Connected, Autonomous Cars)

- ▮ Entwicklung einer Sicherheitsarchitektur für vernetzte autonome Fahrzeuge
- ▮ Sichere C2X-Kommunikation und Datenfusion
- ▮ Sicherheit und Integrität von Bordnetzen

Qualitätsberatung für sichere Software

- ▮ Consulting zur Entwicklung spezifischer Entwicklungsrichtlinien für die Realisierung von sicherheitskritischer Software nach SIL und ISEC
- ▮ Unterstützung bei der Vorbereitung für die Zertifizierung nach Bankenstandards

SIBASE (Sicherheitsbaukasten für eingebettete Systeme)

- ▮ Erforschung des Zusammenspiels von Secure Boot, Secure Update und Secure Communication mit dem Ziel, eine Langzeitabsicherung von kritischen Systemen zu gewährleisten
- ▮ Umsetzung der Konzepte in einem Automotive-Demonstrator mit Hardware Security Module (HSM) am Beispiel von Firmware Over-the-Air Update

SIMPL(Secure IoT Management Platform)

- ▮ Entwicklung einer sicheren Managementlösung für IoT-Systeme
- ▮ Entwicklung eines unabhängigen Security-Layers, der eine sichere Kommunikation zwischen IoT-Geräten gewährleistet
- ▮ Entwicklung jeweils eines Demonstrators für den beispielhaften Anwendungsfall Capacity Sharing

Weitere Projektbeispiele...

Testautomatisierung für Smart Metering-Systeme

Analyse, Verbesserung des aktuellen Testprozesses sowie Einführung von Continuous Integration in der Entwicklung von Smart Meters für Strom und Wasser

ETIBLOGG (Energy Trading via Blockchain in the local green grid)

- ▮ Entwicklung einer Plattform (Blockchain Device) für den Peer-to-peer Energiehandel über Blockchain
- ▮ Weiterentwicklung der eigenen Linuxplattform durch ein Secure Update Framework mit Imagepersonalisierung
- ▮ Entwicklung eines stufenweisen Demonstrators in einem Testumfeld hin zu Realsystem in einem Gewerbepark

Trusted Platform Module (TPM)

- ▮ Entwicklung von Trusted Computing Applications
- ▮ Entwicklung von Tools zur Funktions- und Ausgangsprüfung von hochsicherheitsfesten Kryptoprozessoren (TPMs)
- ▮ Treiberentwicklung für Linux und U-Boot

Tooling für Verbrauchsdatenerfassung

Software-Entwicklung für die exakte und sichere Abrechnung angefallener Kosten von Heizung sowie Warm- und Kaltwasser im privaten und gewerblichen Bereich

Validierung von Kryptoalgorithmen

- ▮ Umsetzung komplexer Algorithmen wie DES und SHA in VHDL
- ▮ Anschließende Verifikation und Validierung per Softwaresimulation und Freigabevorbereitung für den Kunden