Embedded Security

MIXED MODE

technik.mensch.leidenschaft

SECURITY

Wie sicher sind Ihre Embedded Systeme?

Bedrohungen für Ihre Systeme:

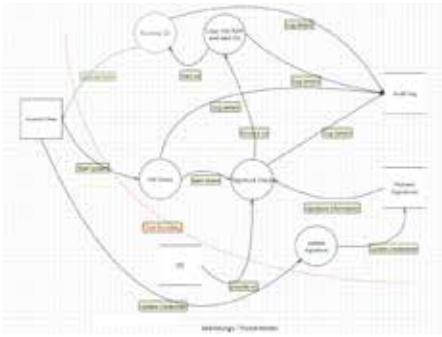
- Ausspionieren von Daten, Intellectual Property und Know-how
- Unberechtigte Zugriffe auf Informationen und Abläufe
- Manipulation von Daten, Programmen und Speichern
- Einspielen gefälschter Updates
- Blockieren der Infrastruktur durch gezielte Überlastung

Durch die immer stärkere Vernetzung und die Verbreitung des „Internet of Things" werden auch Embedded Systeme angreifbar. Aber wie dagegen absichern? Wie erfolgt die Umsetzung in der Praxis? Wie viel Sicherheit ist genug? Wie kann auch die zukünftige Sicherheit Ihrer Systeme gewährleistet werden?

Wir klären Sie über die Gefahren auf und unterstützen Sie bei der Lösung dieser Probleme mit unserer Kompetenz in der Realisierung sicherer Embedded Systeme, die wir in mehr als zehn Jahren aufgebaut haben.

Informationssicherheit durch sichere Systeme und sichere Software

Security Engineering – Security beginnt schon beim Entwurf



- **Security Awareness**
- **Ermitteln der Sicherheitsanforderungen**
- **Festlegen von Security Levels**
- **Bedrohungsanalyse** (Threat Modeling)
- **Secure Design Patterns & Principles**
- **Sichere Systemarchitektur**
- **Einsatz von Security Building Blocks**
- **Security-Erweiterung** bei vorhandener Hardware
- **Design- und Code-Reviews/Assessments**

Sichere Kommunikation und Vernetzung – nicht ohne Verschlüsselung und Signatur

- **Verschlüsselung** durch Anwendung von bewährten **Kryptographie-Algorithmen** (symmetrisch, asymmetrisch)
- **Vertrauen durch digitale Signaturen**
- Einbindung von Embedded Devices in eine **Public Key Infrastruktur**
- **Authentifizierungs- und Autorisierungsmechanismen** (für Personen, Embedded Systeme, Prozesse)
- **Security-Erweiterung** vorhandener Kommunikationsprotokolle
- Sichere Integration in Ihre **IT**-Infrastruktur und Vernetzung mit der **Cloud**
- Sicheres **Software Defined Networking**

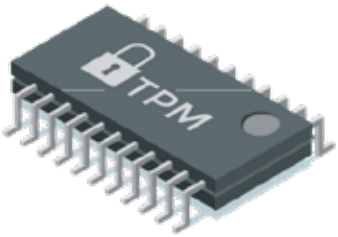
Sichere Software – Schwachstellen vermeiden

- **Programmierstandards** z.B. MISRA, SEI CERT C
- **Design Rules**
- **Statische Codeanalyse** z.B. mit SonarQube, cppcheck, Clang
- **Techniken für sicheres Programmieren** (Input-Validierung, Output-Sanitisierung, geprüfte SW-Bibliotheken, minimale Rechte)
- **Logging und Audit**
- **Secure Boot, Secure Update und Secure Methods** (z.B. Virtualisierung, Firewall, Segmentierung)
- **Separation Micro Kernel**

Sichere Systeme – mit Hardware-Unterstützung

- **Hardware-Unterstützung** durch ein **Secure Element** wie z.B. ein **HSM** (Hardware Security Modul), ein **TPM** (Trusted Platform Module) oder **SHE** (Secure Hardware Extension)
- **Secure Memory, Secure Storage** (z.B. für Credentials)
- **Trusted Execution Environment** (Arm® TrustZone®, OP-TEE, TF-A/M)
- **Smart Cards**

Sicherheitsnormen – wir informieren Sie



- **Common Criteria – ISO/IEC 15408, BSI PP**
- **IT-Grundschutz ISO 27001**
- **ISO/IEC 62443-4-x**
- **DIN 27072**
- **PSA Certification – Level 1**
- **Mixed Mode ist Mitglied im Sicherheitsnetzwerk München**

ÜBER UNS

technik.mensch.leidenschaft

Seit 1990 bieten wir unseren Kunden professionelles Embedded & Software Engineering. Mixed Mode beschäftigt derzeit über 100 Spezialisten.

Ob Sie individuelle Lösungen benötigen, qualifizierte Experten für Ihr Team suchen oder innovative Ideen und Technologien für Ihre Projekte benötigen – greifen Sie auf unser komplettes Wissensspektrum und unsere Erfahrung zurück.

Qualität und beste Kundenzufriedenheit bilden die Basis für eine erfolgreiche und langfristige Zusammenarbeit.

Unsere Kunden sind Global Player und innovative mittelständische Unternehmen aus allen Schlüsselbranchen. Sie schätzen uns als zuverlässigen Partner gemäß unserem Motto:

Unsere Kernkompetenz ist technik. Der mensch steht bei uns im Mittelpunkt. Wir machen unseren Job mit leidenschaft.