Embedded Security

Das Technologieunternehmen ITK Engineering stellt sich den Sicherheitsherausforderungen der Zukunft.

Seit jeher ist dem Menschen die Sicherheit ein elementares Grundbedürfnis, welches sich über alle Lebensbereiche erstreckt. Das gilt auch für die Fahrt in einem Fahrzeug.

In den letzten 30 Jahren wurde eine Vielzahl von Assistenzsystemen entwickelt, die zum einen die Unfallschwere mindern und zum anderen Unfälle völlig verhindern sollen. Diese elektronischen Systeme greifen teils aktiv in das Fahrgeschehen ein, beispielsweise durch das Einleiten einer Notbremsung in Gefahrensituationen, und unterliegen bei der Entwicklung der Norm der Funktionalen Sicherheit, der ISO 26262.

Je größer der Eingriff in das Fahrgeschehen, desto notwendiger ist eine umfassende Analyse der Verkehrssituation. Daher findet zunehmend eine Vernetzung zwischen dem Fahrzeug und seiner Umwelt statt. Diese Car-2-X-Kommunikation stellt neben dem Sicherheitsgewinn durch zusätzliche Umgebungsdaten jedoch gleichzeitig ein Sicherheitsrisiko dar. Das Fahrzeug ist nun nicht mehr nur physischen Fremdzugriffen wie Diebstahl ausgesetzt, sondern wird zunehmend ein Ziel für Hacker, die Fahrzeugdaten ausspähen und manipulieren können. Durch diese Öffnung der Systeme muss neben Safety in Zukunft auch der Aspekt der Security in der Entwicklung verstärkt berücksichtigt werden.

Security Engineering

Es gibt Veröffentlichungen von Studien, in denen Angriffe bereits erfolgreich durchgeführt wurden. Hierbei konnte über ein manipuliertes Lied auf einer CD die Telematikeinheit des Fahrzeugs angegriffen und dadurch Zugang zum CAN-Bus erlangt werden. Zugriffe auf kritische Systeme, wie z.B. die Bremsen, waren somit möglich (Quelle: Checkoway, S. et al: Comprehensive Experimental Analyses of Automotive Attack Surfaces. USENIX Security Symposium, 2011). Um das Fahrzeug gegen Angriffe zu schützen reicht es nicht aus, einzelne Elemente abzusichern, wie beispielsweise durch eine Firewall. Wurde z.B. einmal der Schlüssel zur Absicherung der Kommunikation - ähnlich der Verschlüsselung einer E-Mail - gefunden und darüber der Zugang zum Fahrzeug erlangt, kann immer wieder mit weitaus geringerem Aufwand in das System eingedrungen werden.

Security als Schlüssel zum sicheren, vernetzten Fahrzeug.

Da Angreifer sich das Angriffsziel aussuchen können, hängt die Security des Systems immer am schwächsten Glied. Eine lückenlose Verwendung von Security-Bausteinen, wie z.B. von Gefährdungsbaumanalysen oder Hardware Security Modulen (HSM), ist daher notwendig. Der Einsatz dieser Bausteine hängt ab von den jeweiligen Sicherheitszielen, wie Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit. Security Engineering muss somit bereits in frühen Entwicklungsphasen verankert werden, um Wissen und Daten sowie Schutz vor Manipulation zu gewährleisten.

In praktischen Demonstrationen und Implementierungen beschäftigt sich ITK Engineering mit Methoden, die in Abwesenheit von HSM, Schlüssel aus dem Hauptspeicher von Microcontrollern zu extrahieren. Neben der Anwendung von Security-Bausteinen befasst sich ITK Engineering intensiv mit Security Engineering und Embedded Krypto-Benchmarking. Embedded Krypto-Benchmarking ist ein Messverfahren, um die Leistung von Systemen und Algorithmen nach bestimmten Kriterien zu vergleichen.

Das Unternehmen

Die Unternehmensstruktur von ITK Engineering besteht aus drei Säulen: Projekte, Mitarbeiter und Innovation. Der Bereich Innovation teilt sich in zwei Fachbereiche, die in Vorentwicklungsprojekten neuartige Methoden und Systemlösungen entwickeln und schulen. Dies ermöglicht die frühzeitige Auseinandersetzung mit neuen, komplexen Herausforderungen, wie dem Security Engineering. Zusätzlich greift ITK Engineering auf eine langjährige Projekterfahrung in der Entwicklung von Fahrerassistenzsystemen zurück, wie z.B. beim vorausschauenden Abstandregeltempomaten und Ausweichassistenten. Besonders zum Tragen kommen hierbei das fundierte Wissen im Bereich der Funktionalen Sicherheit, der Algorithmenentwicklung sowie der Regelungstechnik.

ITK Engineering ist ein gründergeführtes, international agierendes Technologieunternehmen mit namhaften Kunden aus der Automobilindustrie, Medizintechnik und Luftfahrt. Neben maßgeschneiderter Beratung und Entwicklungsunterstützung liefert das Unternehmen Systemlösungen in den Bereichen Software Engineering, Embedded Systems, modellbasierte Entwicklung und Test, Regelungstechnik sowie Signalverarbeitung.

Um das Wissen im Bereich Entwicklung von System-/Embedded Software sowie Safety und Zertifizierung kontinuierlich mit OEMs, anderen Entwicklungspartnern und Komponetenlieferenaten zu erweitern, engagiert sich ITK seit Mai 2013 in SafeTRANS.

www.itk-engineering.de

SHORTCUTS: ITK Engineering AG

Unternehmen:	ITK Engineering AG
Zentrale:	Rülzheim
Niederlassungen:	München, Stuttgart, Marburg, Braunschweig, Frankfurt, Graz, Tokyo, Detroit
Geschäftsfelder:	Automobil, Luftfahrt, Medizintechnik, Bahn
Gründungsjahr:	1994
Mitarbeiter:	über 700

Fragen an Matthias Gemmar, Fachbereichsleiter Methoden:

Wie beurteilen Sie die Auswirkungen von Security auf Safety im Entwicklungsprozess?

Um Safety zu gewährleisten, muss Security sichergestellt werden. Damit wird verhindert, dass notwendige Safetymechanismen manipuliert werden können. Auch wenn die Quantifizierbarkeit bei Security ungleich schwerer ist, sind sich die jeweiligen Sicherheitsanalysen vom Charakter her ähnlich, wobei sich die technischen Mechanismen unterscheiden. Genau wie bei Safety bietet ein solider Qualitätssicherungsprozess die Grundlage. Ein enges Zusammenspiel zwischen Qualitätsmanagement, Safety und Security ist daher unabdingbar.

Wie geht ITK Engineering beim Krypto-Benchmarking vor?

Krypto-Bechnmarking auf Embedded Targets dient der Vergleichbarkeit der Effizienz von Krypto-Algorithmen. Wir vergleichen hierbei die unterschiedlichen Algorithmen auf identischen Systemen und unter identischen Ausführungsbedingungen. Ein entscheidendes Kriterium für die Effizienz auf Embedded Targets ist der Speichbedarf.

Lassen sich Security-Anforderungen und -Lösungen aus Automotive-Anwendungen in die Medizintechnik und Luftfahrt übertragen?

Ja und umgekehrt. Herzschrittmacher mit Funkschnittstelle, immer stärker funktional vernetzte OPs und (mobile) Applikationen mit Zugriff auf Patientendaten bieten die gleichen Herausforderungen wie ein vernetztes Fahrzeug - insbesondere bei den Methoden und Prozessen.