IAA / New Mobility World 2017: Kaspersky Lab und AVL Software and Functions GmbH präsentieren Secure Communication Unit für Connected Cars

Moskau/Ingolstadt/Frankfurt, 13. September 2017

Hersteller von vernetzten und autonomen Fahrzeugen stehen vor zahlreichen Herausforderungen hinsichtlich der Cybersicherheit. Kaspersky Lab und die AVL Software and Functions GmbH präsentieren daher im Rahmen der New Mobility World auf der IAA 2017 in Frankfurt die neue Plattform Security Communication Unit (SCU) [1]. Die Sicherheitslösung zur Umsetzung eines Security-by-Design-Ansatzes für Connected Cars steht aktuell als Prototyp zur Verfügung und demonstriert die Möglichkeiten einer störungsfreien Kommunikation des Fahrzeugs, seiner Komponenten und der externen vernetzten Infrastruktur.

In jeder Fahrzeuggeneration finden sich neue, intelligente Technologien für Fernwartung, Telematik, automatisches und autonomes Fahren, ferngesteuerte Fahrerassistenzsysteme oder Infotainment. Durch den Einsatz elektromechanischer Antriebselemente erfolgt die Fahrzeugkontrolle inzwischen über komplexe, cyberphysische Systeme mit zahlreichen Sensoren, Kontrollelementen, Anwendungen, Teilnetzen und Kommunikationsmodulen, die in Kontakt zu anderen Fahrzeugen und dem Umfeld stehen. Die Funktionen lassen sich digital von außen steuern. Doch genau das macht vernetzte Fahrzeuge zunehmend auch zum Ziel von Cyberangriffen [2].

„Da moderne Fahrzeuge immer komplexer und vernetzter werden, überrascht es nicht, das bei Kunden und Herstellern inzwischen auch Bedenken bezüglich der Cybersicherheit aufkommen“, sagt Andrey Doukhvalov, Head of Future Technologies and Chief Security Architect bei Kaspersky Lab. „Neben all den neuen Möglichkeiten und Vorteilen, die Fahrzeugsysteme bieten, gibt es auch einen Bedarf, Fahrzeugsysteme cybersicher zu machen. Unser Prototyp für die sichere Fahrzeugkommunikation ist ein großer Schritt nach vorne und garantiert, dass die vorteilhaften Möglichkeiten der Konnektivität nicht an Sicherheitsfragen scheitern.“

SCU: Security-by-Design

Die Prüfung sämtlicher IT-Systeme eines Fahrzeugs auf vorhandene Bugs, Backdoors oder Schwachstellen in der Software-Architektur wird immer aufwendiger. Gründe dafür sind immer mehr Drittanbieter-Anwendungen, die zunehmende Komplexität und immer schnellere Update-Zyklen, die auch remote ausgeführt werden können. Die neue Secure Communication Unit (SCU)

setzt im Hinblick auf Cybersicherheit bereits im Entwicklungsprozess vernetzter Fahrzeuge an, unabhängig von eventuell vorhandener Software oder Systeme von Drittanbietern. SCU ist mit unterschiedlichen im Fahrzeug vorhandenen Teilnetzen oder Gateways verbunden und arbeitet als Steuereinheit für den sicheren ein- und ausgehenden Datenverkehr. Enge Sicherheitsrichtlinien sowie eine Trennung untereinander verhindern den ungewollten Kontakt zwischen einzelnen Fahrzeugkomponenten und sichern eine störungsfreie Netzwerkkommunikation innerhalb des Fahrzeugnetzwerks.

KasperskyOS als Basis

SCU ist eine zuverlässige Software-Plattform, deren Komponenten dem Trustworthy-by-design-Ansatz folgen. Das auf Microkernel basierende und proprietäre Betriebssystem KasperskyOS [3] wurde nach bewährten, sicherheitsgetriebenen Prinzipien entwickelt und eignet sich speziell für den Einsatz innerhalb eingebetteter Systeme mit strikten Cybersicherheitsanforderungen. KasperskyOS verhindert die Ausführung nicht dokumentierter Funktionalität und minimiert damit das Risiko von Cyberangriffen. Selbst wenn nicht autorisierter Code in das System gelangen sollte, könnte er nicht ausgeführt werden, denn jede nicht dokumentierte Funktionalität ist standardmäßig unzulässig.

Weitere Komponenten wie Kaspersky Security System integrieren eine Security Policy Engine, die den speziellen Bereich der Interaktion zwischen verschiedenen Komponenten und einem Trusted Channel Framework definiert. Dies geschieht über Kryptoalgorithmen sowie über Sicherheitsdienste, die auf den Hardwarefähigkeiten basieren.

Der in Frankfurt vorgestellte SCU-Prototyp wurde beispielhaft im Rahmen der Architektur ARMv7 implementiert und erfordert 128 MB RAM sowie IOMMU. In Absprache mit den Herstellern können fallweise auch andere Hardware-Plattformen unterstützt werden.

Die Plattform versteht sich als Framework für die Entwicklung eigener Anwendungen. Fahrzeughersteller können für ihre Fahrzeuge eine eigene SCU implementieren, welche die spezifischen Hardware- und weitere Softwarekomponenten sowie den jeweiligen Produktionsprozess berücksichtigt. SCU steht allen OEMs, ODMs, Systemintegratoren und Software-Entwicklern weltweit zur Verfügung.

[1] siehe auch Abbildung unter:
http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_SCU_infographics_ENG__1_.jpg

[2] siehe auch Abbildung unter:
http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_Grafik_Cyberbedrohungen_Connected_Cars.jpg

[3] https://os.kaspersky.com/

Nützliche Links:

- Kaspersky-Infografik „How to make a connected car truly secure“: http://newsroom.kaspersky.eu/fileadmin/user_upload/de/Downloads/PDFs/Kaspersky_SCU_infographics_ENG__1_.jpg
- Pressemitteilung „Kaspersky Lab und AVL Software and Functions GmbH kooperieren bei der Entwicklung für Cybersicherheit in der Automobilindustrie“: http://newsroom.kaspersky.eu/de/texte/detail/article/kaspersky-lab-und-avl-software-and-functions-gmbh-kooperieren-bei-der-entwicklung-fuer-cybersicherhe
- Kaspersky-Blog „Vernetzte Autos: Security by Design”: https://kas.pr/dv5a

Über AVL

AVL is the world's largest independent company for the development, simulation and testing technology of powertrains (hybrid, combustion engines, transmission, electric drive, batteries and software) for passenger cars, trucks and large engines. AVL has more than 8,600 employees all over the world. In 2016, sales revenues reached EUR 1.4 billion.

Über Kaspersky Lab

Kaspersky Lab ist ein global agierendes Cybersicherheitsunternehmen, das im Jahr 2017 sein 20-jähriges Firmenjubiläum feiert. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky Lab ist Basis für Sicherheitslösungen und -Services zum Schutz von Unternehmen, kritischen Infrastrukturen, staatlichen Einrichtungen sowie Privatanwendern weltweit. Das umfassende Sicherheitsportfolio des Unternehmens beinhaltet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services zur Verteidigung vor komplexen und aufkommenden Cyberbedrohungen. Mehr als 400 Millionen Nutzer und 270.000 Unternehmenskunden werden von den Technologien von Kaspersky Lab geschützt.

Weitere Informationen zu Kaspersky Lab finden Sie unter http://www.kaspersky.com/de/. Kurzinformationen erhalten Sie zudem über www.twitter.com/Kaspersky_DACH und www.facebook.com/Kaspersky.Lab.DACH. Aktuelles zu Viren, Spyware, Spam sowie Informationen zu weiteren IT-Sicherheitsproblemen und -Trends sind unter https://de.securelist.com/ und auf dem Kaspersky-Blog auf http://blog.kaspersky.de/ abrufbar.

Redaktionskontakt:

Berkeley Kommunikation GmbH
Florian Schafroth
florian.schafroth@berkeley.global
Tel.: +49-89-7472-62-43
Fax: +49-89-7472-62-17

Kaspersky Labs GmbH
Stefan Rojacher
stefan.rojacher@kaspersky.com
Tel.: +49-841-98-189-325
Fax: +49-841-98-189-100

Landwehrstraße 61
80336 München

Despag-Straße 3
85055 Ingolstadt