Mehr Sicherheit für die Sicherheit

AUTOREN

Dr. Jan Pelzl ist Geschäftsführer der **ESCRYPT GmbH**.

Dr. Thomas Wollinger ist Geschäftsführer der **ESCRYPT GmbH**.

Car-2-Car-Kommunikation vor Fehlern und Missbrauch schützen

Car-2-Car-Kommunikation ist die nächste große Evolutionsstufe des Straßenverkehrs. Indem die Fahrzeuge der Verkehrsteilnehmer Nachrichten und Warnungen austauschen, lassen sich Gefahren im Vorfeld erkennen und der Verkehrsfluss besser lenken. Doch die dafür eingesetzten offenen Kommunikationsschnittstellen müssen gegen unautorisierten Zugriff abgesichert werden. Hersteller, Forschungs- und Pilotprojekte arbeiten intensiv an Schutzmaßnahmen und nutzen etablierte Sicherheitsstrategien aus der Informationstechnik – und ESCRYPT ist vorne mit dabei.

Mit Car-2-Car (C2C)- und Car-2-X (C2X)-Kommunikation haben es Hersteller und OEMs in der Hand, den Fahrer mit intelligenter Technik zu unterstützen und so Unfälle zu vermeiden. Zukünftig tauschen die Verkehrsteilnehmer Warnungen und Nachrichten automatisiert und direkt aus. Das Institut für Wirtschaft und Verkehr an der Technischen Universität Dresden ist davon überzeugt, dass sich beispielsweise staubedingte Reisezeitverzögerungen mehr als halbieren ließen, wenn nur allein zehn Prozent der Fahrzeuge C2C-Kommunikation unterstützen würden*.

Für eine Anwendung, die potentiell Eingriffe in die Fahrdynamik vornimmt, ist das Vertrauen der Anwender das höchste Gut. Integrität und Vertraulichkeit der ausgetauschten Nachrichten müssen jederzeit garantiert sein. Dem stehen die offenen und drahtlosen Schnittstellen der C2C-Kommunikation entgegen.

Wenn Nachrichten per Nahbereichsfunk gesendet und empfangen werden, kann grundsätzlich jeder eine entsprechende Sende- und Empfangseinheit aufstellen und an der Kommunikation teilnehmen. Drehund Angelpunkt ist die Zertifizierungsstelle (CA – Certificate Authority), ein Bestandteil jeder Public-Key-Infrastruktur (PKI). Hier bietet ESCRYPT attraktive Lösungen mit den notwendigen kryptographischen Schlüsseln nach dem neuesten Stand der Technik. Überall, wo sich elektronische Embedded Systeme authentifizieren, freischalten oder sicher kommunizieren, kann die ESCRYPT „Key Management Solution" zum Einsatz kommen. Sie kann vom Kunden selbst oder als „Managed Service" vollständig durch ESCRYPT betrieben werden.

Herausforderungen

Die hohe Mobilität der Teilnehmer bedingt kurze Verbindungszeiten. Eine Kommunikation mit der Infrastruktur kann nicht vorausgesetzt werden. Digitale Signaturen, ein wichtiger Bestandteil des C2C-Schutzkonzepts, müssen daher anders implementiert werden als bei klassischen IT-Anwendungen. So sind sehr lange Zertifikatslaufzeiten notwendig, denn es kann keine Verbindung zu einem System garantiert werden, das in der Lage wäre, Zertifikate auszustellen, zu prüfen und für gültig oder ungültig zu erklären. Um Bewegungsprofile von Fahrzeug und Fahrer zu verhindern, müssen die Zertifikate pseudonymisiert sein.

On-Board-Units sind IT-Systeme

In der C2C-Kommunikation kommen zumindest in Teilbereichen TCP/IP-Protokolle zum Einsatz. Davon profitieren auch Angreifer, die gut dokumentierte Paketformate und zahlreiche Tools nutzen können. Forschungsprojekte wie PRESERVE oder SEVECOM versuchen, einen möglichst universellen Ansatz zur Abwehr zu formulieren. Basierend auf den Schutzzielen Integrität, Verfügbarkeit und Authentizität, werden die einzelnen Systeme, Daten, Kommunikationsverbindungen und Funktionen hinsichtlich ihrer Schutzwürdigkeit analysiert. Das Ergebnis sind Schutzbedarfskategorien, die zusätzlich Motivation und Möglichkeiten der Angreifer in Betracht ziehen. Durch die feine Untergliederung können Schutzmaßnahmen sehr gezielt nach Aufwand und Wirkung eingesetzt werden.

Hersteller, Forschungsprojekte und Organisationen wie das Car-2-Car Communication Consortium (C2C-CC) nehmen sich seit mehreren Jahren dieser Aufgabenstellung an. Im Februar 2014 wurden in Europa grundlegende Standards für den Datenaustausch zwischen vernetzten Fahrzeugen durch das European Telecommunications Standards Institute (ETSI) und das European Committee for Standardisation (CEN) geschaffen. Die Gremien verständigten sich unter anderem auf Funkfrequenzen und Datenformate und kooperierten mit den zuständigen Gremien in den USA und Japan.

*) Quelle: www.berliner-zeitung.de