Christiane Schulzki-Haddouti

Schlüsselgewalt

Wer erhält den Schlüssel zum vernetzten Auto?

Kryptografische Lösungen bestimmen, wer den Schlüssel für das vernetzte Auto in der Hand haben wird. Automobil-Hersteller und Staat ringen derzeit darum, wie diese Lösungen aussehen sollen. Die Interessen der Fahrzeughalter spielen dabei offenbar kaum eine Rolle.

Die europäische Datenschutzreform verlangt im Interesse der Bürger, Autobesitzer und Fahrer „Privacy by Design". Die aktuelle Diskussion um Sicherheitskonzepte für das „vernetzte Auto" weist aber in eine andere Richtung. Solche Fahrzeuge erzeugen stündlich zwischen 20 und 24 Gigabyte Daten, sagt Gabriel Seiberth von der Unternehmensberatung Accenture. Die Automobilbranche sei daher auf der Suche nach Geschäftsmodellen, „damit die Daten nicht einfach anfallen und wieder verpuffen". In zehn Jahren sollen solche Geschäftsmodelle Umsätze in Milliardenhöhe generieren.

Ein aktueller Fall aus Baden-Württemberg zeigt jedoch, dass dies an den Datenschutzsorgen der Kunden scheitern könnte. Ingo Scherzberg und seine Frau hatten im Verkaufsgespräch die Übertragung von Ortsdaten aus ihrem Auto strikt abgelehnt. Erst nach der Auftragsbestätigung wurde Scherzberg bei der Lektüre der Broschüre „Ihr Weg zu Mercedes connect me" klar, dass das Kommunikationsmodul, über das die Ortsdaten übertragen werden, nicht ausgebaut werden würde.

„Ganz aus" war es bei ihm, als er in den Unterlagen zur Informationssicherheit von eCall auch noch Hinweise auf mögliche Hackerangriffe entdeckte. Den Versicherungen von Daimler, es würden gegen seinen Willen keine Daten übertragen, konnte er keinen Glauben schenken: „Der Staat hat die Speicherung von Telefondaten durchgesetzt und das Bankgeheimnis ausgehebelt, zweifellos wird er auch die Herausgabe der Ortsdaten fordern." Nachdem Scherzberg heftig protestierte, löste Daimler den Kaufvertrag auf.

Zwiespalt

Die Hersteller zeigen sich hin- und hergerissen. Einerseits betont etwa Volkswagen-Chef Martin Winterkorn, dass das Auto nicht zur „Datenkrake" werden dürfe, andererseits machen die Hersteller in ihrem Datenschutz-Positionspapier einen weiten Bogen um das Prinzip der Datensparsamkeit. Hierarchische Sicherheitsarchitekturen für den Datenaustausch zwischen Autos (Car-to-Car) sowie zwischen Autos und Infrastruktur (Car-to-X) sorgen überdies nicht unbedingt für Vertrauen.

Mit Car-to-Car-Kommunikation lässt sich beispielsweise unterwegs und in Echtzeit die Parkplatzsuche organisieren. Oder man übermittelt Unfall- und Stauwarnungen ortsbezogen, um die Navigation zu verbessern. Über „Cooperative Awareness Messages" können während des Fahrens Warnungen vor Endpunkten von Staus, Hinweise für das Überqueren von Kreuzungen und „Grüne Wellen" übermittelt werden. Dies alles ermöglicht in einem weiteren Schritt auch teilautonomes Fahren.

Mit Car-to-Infrastructure-Kommunikation kann die Ampel mitteilen, wann sie rot wird und das System kann die optimale Geschwindigkeit des Fahrzeugs ermitteln. In Echtzeit lassen sich Informationen über stark und schwach befahrene Strecken ermitteln. Auch könnten Mautgebühren erhoben werden, ohne dafür Erfassungsgeräte zu installieren.

Immer mehr Städte haben Probleme mit Feinstaub, Kohlendioxid und knappem Parkraum. Die ließen sich über öffentliches Carsharing lösen, quasi als neues öffentliches Nahverkehrs-System. Das schlagen die Analysten der Brookings Institution vor, einer US-amerikanischen Denkfabrik für Politik im öffentlichen Bereich. Die Stadt könnte dabei mit digitalen Schlüsseln steuern, welche Fahrzeuge in die Stadt fahren und dort parken dürfen. Vielleicht landet das Smart-City-Geschäft aber auch in den Händen der Autohersteller, die dann steuern, wer wo fahren darf.

Bedenken

Während die Geschäftsmodelle schon einigermaßen ausformuliert sind, ist die technische Roadmap wegen organisatorischer Fragen noch offen. Weitgehend ungeklärt ist die Gretchenfrage hinter den neuen Geschäftsmodellen: Wer hat Zugriff auf die Fahrzeugdaten? Und wer hält den Schlüssel zu den Daten in der Hand?

Die gegenwärtigen Konzepte zu Sicherheitsstandards für vernetzte Autos verwenden die klassische Public-Key-Infrastruktur (PKI). Sie sollen verhindern, dass unberechtigte Dritte die Daten manipulieren. Bei einer traditionellen PKI ist die Schlüsselgewalt hierarchisch geregelt: Der Nutzer muss dem Verwalter vertrauen, dass dieser die Schlüssel diebstahlsicher verwahrt und nicht missbraucht.

Schon heute haben die Autofahrer keine Kontrolle über das Sammeln und Auswerten von Verkehrsdaten, die mit ihren Wagen erzeugt werden. Damit könnten umfangreiche Bewegungsprofile und abgeleitet hiervon auch Persönlichkeitsprofile erstellt werden. Die Auto-Hersteller betonen, dass die Daten nur mit Zustimmung der Kunden verwendet werden. Auch behaupten sie, die Datenauswertung erfolge anonym. Doch eine unabhängige Überprüfung dieser Anonymität etwa seitens einer Datenschutz-Aufsichtsbehörde ist bislang nicht bekannt.

Eine Alternative wären sogenannte attributbasierte Berechtigungsnachweise (ABCs). Damit teilt das Auto einem anderen Auto oder der Infrastruktur nur das für den Dienst

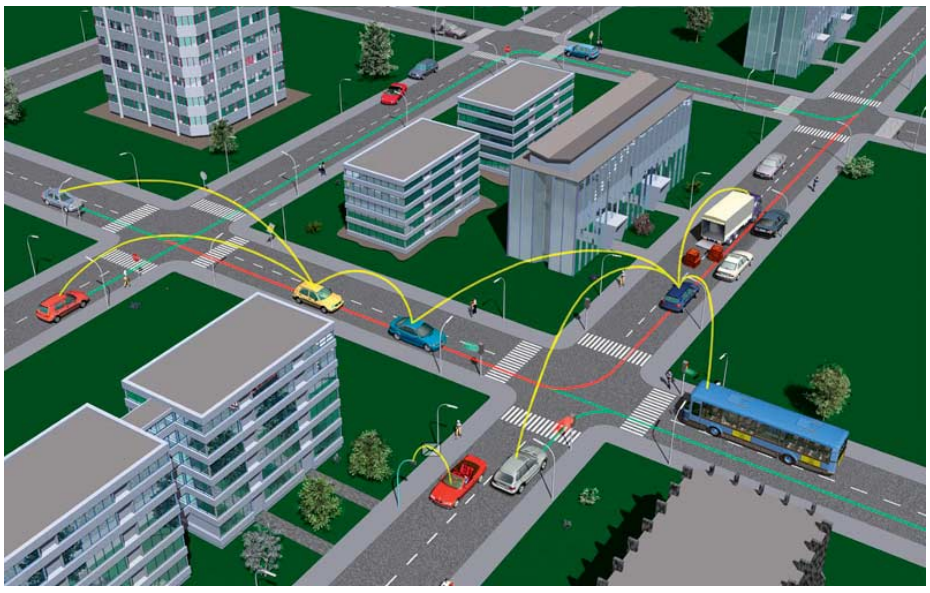

Bild: Car 2 Car Communication Consortium

Vernetzte Autos tauschen eine Menge verschlüsselter Daten aus. Die Art der Verschlüsselung entscheidet darüber, ob die Privatsphäre von Besitzern und Fahrern dabei geschützt wird.

notwendige Attribut mit, etwa Geschwindigkeit und Richtung, ohne sich gleichzeitig zu identifizieren.

Skeptisch stimmt ein Bericht des dänischen Sicherheitsforschers Stephan Engberg, der im europäischen Standardisierungsgremium ETSI an der Entwicklung des Standards für die Kommunikationsarchitektur Intelligenter Transport-Systeme (ETSI EN 302 665) mitgewirkt hatte. Er sagt, dass die Hersteller das klassische PKI-Konzept bevorzugen: „Die Hauptagenda besteht darin, die Auto-Kommunikation nach Willen der Automobilhersteller und ihrer Partner zu gestalten, ohne dabei Fragen wie Sicherheit, Effektivität und Rechtslage ausreichend zu berücksichtigen."

Engberg betont, man könne mit ABCs sowohl Tracking verhindern als auch Mechanismen für die Kriminalitätsbekämpfung einbauen, die eine Re-Identifizierung erlauben. Doch damit nicht genug: Man kann für Unfälle punktuelles Tracking ermöglichen, aber gleichzeitig Tracking über größere Distanzen und längere Zeiträume verhindern. Er betont: „Legitime Geschäftsmodelle und Sicherheitsanforderungen können immer mit Privacy by Design ermöglicht werden. Es sind nur die nicht-legitimen Modelle, die Überwachungsfunktionen verlangen."

Allerdings kosten ABCs etwas mehr als herkömmliche PKIs – und die Autohersteller schauen auf jeden Cent. Außerdem funktionieren damit die anvisierten Geschäftsmodelle womöglich nicht, sagt Accenture-Berater Seiberth. Er empfiehlt den Herstellern, bei Google zu lernen: Die Kunden geben freiwillig Daten von sich preis, wenn sie dafür eine Gegenleistung erhalten.

Forschungsprojekt

Im Car 2 Car Communication Consortium arbeiten europäische Autohersteller, Zulieferer und die IT-Industrie an Spezifikationen, um sie beim ETSI zur Standardisierung einzureichen. Das Konsortium betreibt auch Forschungsprojekte wie Converge, das ein Sicherheitskonzept mit Pseudonymen und Attributen nutzt. Dabei identifiziert ein Langzeit-Zertifikat das Fahrzeug. Es wird dafür verwendet, die Zertifikate für die Pseudonyme abzuholen, die die Kommunikation absichern. Sie gelten nur für einige Wochen.

Die Stelle, die das Langzeit-Zertifikat ausstellt, weiß nicht, welche Pseudonyme vergeben werden, und die Stelle, die Pseudonym-Zertifikate vergibt, weiß nicht, für welche Identität sie diese ausstellt. „Erst wenn beide Stellen zusammenarbeiten, lässt sich die Pseudonymisierung aufheben. Für eine Re-Identifizierung sind aber rechtliche Voraussetzungen notwendig", sagt Daniel Angermeier vom beteiligten Fraunhofer-Institut AISEC. Auch könne man das Langzeit-Zertifikat zurückrufen, was das Abholen neuer Pseudonyme unterbindet.

Der Backend-Server, der die Dienste des Converge-Projekts verwaltet, nutzt auch eine PKI. Dabei lassen sich die Dienste pseudonymisiert nutzen, da Attribute den Nutzer legitimieren. „Ob bei Converge wirklich ABCs eingesetzt werden oder andere Arten von Pseudonymen, kann ich nicht genau feststellen", meint aber die neue schleswig-holsteinische Landesdatenschützerin Marit Hansen nach Durchsicht der Unterlagen. Unklar sei auch, wie oft und wie lange die Pseudonyme weiter- und wiederverwendet werden und was dadurch ablesbar wäre.

Innerhalb des Car-2-Car-Konsortiums gilt Converge eher als Nischenprojekt. Die Spezifikation, die bei ETSI vorgeschlagen werden soll, sehe eine klassische PKI vor, sagt Martin Moser, Manager bei der beteiligten Sicherheitsfirma Escrypt. Eine Gruppe aus Automobilherstellern und Zulieferern soll dabei die Root-Zertifizierungsstelle betreiben. Unstimmigkeiten gebe es derzeit noch mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), das eine staatliche Beteiligung in Form einer weiteren Root-Zertifizierungsstelle fordert. Denn noch betreibt die öffentliche Hand die Straßenverkehrs-Infrastruktur, sodass etwa bei vielen Car-to-X-Diensten staatliche Stellen eingebunden werden müssen.

Organisation

Scott Cadzow, der bei ETSI Vorsitzender der ITS Security Group (Intelligente Transport-Systeme) war, erklärt: „Ein Problem besteht darin, dass es bislang noch keine PKIs in der Größenordnung von Milliarden Nutzern gab, die grenzüberschreitend funktionieren müssen." Es sei aber weniger eine technische, denn eine organisatorische Herausforderung festzulegen, wer welchen Zugriff auf die Schlüssel hat.

> ***„Es sind nur die nicht legitimen Geschäftsmodelle, die Überwachungsfunktionen verlangen und Privacy by Design nicht mögen."***
>
> *Stephan Engberg, Sicherheitsforscher*

Wenn dies geklärt sei, werde man auch anfangen, über ABCs nachzudenken, deren Umsetzung noch aufwendiger sei. Die Artikel-29-Gruppe der europäischen Datenschutzbehörden habe bereits Input gegeben. Die Aufsichtsbehörden seien eingeladen worden, sich an der laufenden Diskussion zu beteiligen. Auch gebe es seit diesem Jahr eine „Privacy by Design"-Gruppe bei ETSI, aber daran beteilige sich noch keine deutsche Aufsichtsbehörde.

Die Hersteller werden ihre Geschäftsinteressen gegen den Wunsch der Kunden abwägen, dass ihre Privatsphäre geschützt wird. Das Ergebnis wird bei der Wahl der Verschlüsselung sichtbar werden. Michael Müller, Chef der Beratungsfirma Magility, positioniert sich deutlich: „Weil es letztlich eine Frage der Sicherheit ist, sollte man ABCs nutzen, wenn irgendwie machbar." Sollten die Hersteller zu wenig auf die Interessen ihrer Kunden eingehen, müssen wohl die Datenschutz-Aufsichtsbehörden ihre Zurückhaltung aufgeben und Privacy nach „Stand der Technik" einfordern. (ad@ct.de)