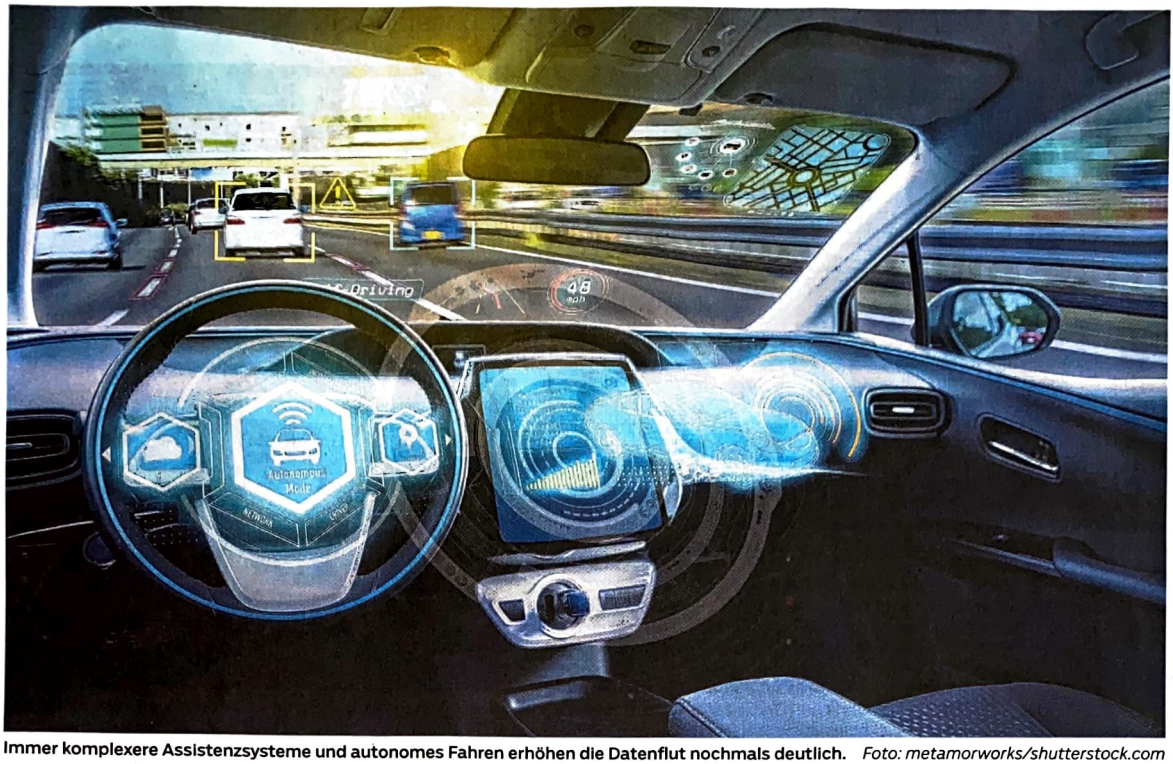


Immer komplexere Assistenzsysteme und autonomes Fahren erhöhen die Datenflut nochmals deutlich. *Foto: metamorworks/shutterstock.com*

# Ferngesteuert: Wenn Hacker das Auto angreifen

**Mobilität** Fahrzeuge sind rollende Computernetzwerke. Und werden dadurch attackierbar. Frank Kargl erforscht, wie böswillige Zugriffe abgewehrt werden können. *Von Stefan Czernin*

**Mehr als zwei Kilometer** Kabel und 100 Steuergeräte: „Ein modernes Auto ist ein Computernetzwerk", sagt Professor Frank Kargl. Er ist Professor für Verteilte Systeme an der Universität Ulm und forscht im Bereich der Fahrzeugkommunikation. Moderne Fahrzeuge sind recht mitteilsam: Die Systeme innerhalb des Fahrzeugs kommunizieren miteinander, das Navigationsgerät holt und sendet Positionsdaten, das Radio spielt die Playlist aus dem Internet. Mit dem Fortschritt im Bereich des autonomen Fahrens nimmt diese Datenflut immer weiter zu: Die Fahrzeuge vernetzen sich untereinander und mit der Verkehrsinfrastruktur, etwa Ampelanlagen.

» SWP-SERIE (7)
**NACHHALTIGE MOBILITÄT**

„Ein Auto war früher ein Inselsystem", sagt Kargl. Es war nicht mit der Außenwelt in Kontakt. Über die Jahre hat es sich immer mehr zu einem rollenden Computernetzwerk entwickelt. Das bringt eine ganze Menge Möglichkeiten und Annehmlichkeiten mit sich. Aber es macht die Fahrzeuge auch angreifbar. Kargl und seine Kollegen arbeiten daran, die Autos vor fremden Zugriffen abzuschirmen. Privatsphäre und Sicherheit nennt er hierbei als die beiden relevanten Aspekte.

„Private Fahrzeuge sind hochgradig personenbezogen." Ein Auto werde im statistischen Schnitt gerade einmal von 1,3 Personen genutzt. Aber wie lässt es sich verhindern, dass zum Beispiel ein Bewegungsprofil von einem Auto erstellt wird, das ständig seine Position, Geschwindigkeit und weitere Daten funkt – unter anderem, um Unfällen vorzubeugen? „Die Fahrzeuge nutzen ein Pseudonym." Und dieses werde zudem alle fünf Minuten gewechselt, so dass selbst eine einzelne Fahrt nicht nachvollzogen werden kann. Um den Schutz der Privatsphäre zusätzlich zu erhöhen, wird auch der genaue Fahrzeugtyp nicht übermittelt. „Wir arbeiten mit Kategorien", erklärt Kargl. Die Information lautet beispielsweise also nicht „Ich bin ein VW Golf", sondern „Ich bin zwischen 4,2 und 4,4 Meter lang".

Auch der juristische Aspekt spielt eine Rolle: „Sollen die Strafverfolgungsbehörden etwa im Fall einer Unfallflucht in der Lage sein, das Pseudonym aufzulösen?", fragt Kargl. „Technisch kann ich beides machen."

Gefährlich wird es, wenn Hacker versuchen, in die Systeme des Fahrzeugs einzudringen und diese zu manipulieren. Dass dies möglich ist, hatte das Internet-Magazin Wired schon 2015 in einem kontrollierten Versuch bewiesen: Computerfachleute setzten einen Jeep Cherokee ferngesteuert in den Graben, der Fahrer konnte nichts dagegen tun. Das

Frank Kargl ist Professor an der Universität Ulm. *Foto: Lars Schwerdtfeger*

Experiment lässt sich immer noch auf Youtube ansehen. Der Hacker, der mit seinem Laptop am Straßenrand steht, ist für moderne Fahrzeuge also durchaus eine Gefahr. „Autos können böswillig manipuliert werden. Man muss sich also dringend über die IT-Sicherheit Gedanken machen", sagt Kargl.

Die Angriffe können sich auf verschiedenen Ebenen ereignen: Hacker können versuchen, über eine Schwachstelle direkt in das Fahrzeugsystem einzudringen. Und so die Bremsen, die Steuerung und weitere Funktionen zu übernehmen. Oder die Angreifer probieren, das Fahrzeug mit falschen Informationen zu täuschen. Und erfinden zum Beispiel einen imaginären Fußgänger, der direkt vor dem Auto auf die Straße tritt, um eine Vollbremsung zu provozieren. Und so einen Unfall auszulösen.

Wie kann ein Fahrzeug eine korrekte Information von einer falschen unterscheiden? Zum einen wird geprüft, ob die empfangene Auskunft überhaupt sinnhaft ist. „Einfach gesagt: Die Information, dass ein Auto mit 500 Stundenkilometern auf mich zufährt, ist wenig plausibel." Auch die Konsistenz der Information wird hinterfragt. Was übermitteln andere Quellen, passt das alles zusammen? „Es geht darum, dem Fahrzeug einen gesunden Menschenverstand beizubringen", fasst Kargl zusammen.

## Professor und Mitglied im Chaos Computer Club

**Kurzbiografie** Privat fährt der 48-Jährige, der in Neu-Ulm wohnt, übrigens kein hochvernetztes Fahrzeug, sondern ein ganz normales Auto. In der Doppelstadt ist er ohnehin am liebsten auf dem E-Bike unterwegs. Frank Kargl stammt aus Unterfranken, ist Informatiker und hat an der Universität Ulm promoviert und habilitiert. Er ist Professor für Verteilte Systeme und Mitglied im Chaos Computer Club, für Fahrzeugkommunikation interessiert er sich seit 2005.