Software unter der *Motorhaube*

TEXT Christian Zimmermann

Hardware tritt in den Hintergrund: Das Fahrzeug der Zukunft wird nicht nur stark von Software geprägt sein, sondern auch Teil eines breit vernetzten, umfassenden Mobilitäts- und Softwareökosystems. Das Software-defined Vehicle bringt viele Vorteile mit sich, aber auch einige Herausforderungen, was Sicherheit und Privatsphäre angeht. Privacy-Enhancing Technologies können helfen, hier den richtigen Gang einzulegen.

Mehr als 100 Steuergeräte sind in modernen Fahrzeugen verbaut, üblicherweise angeordnet in domänenorientierten Fahrzeugnetzen. Das Fahrgefühl und die verfügbaren Funktionen hängen bisher vor allem von der verbauten Hardware ab, deren Potenzial durch Software realisiert wird. Wer hier tiefgreifendere Änderungen vornehmen will, kommt daher oft nicht umhin, auch die Hardware auszutauschen. Dies liegt daran, dass Hardware und Software gemeinsam entwickelt und nach Beginn der Produktion kaum noch verändert werden.

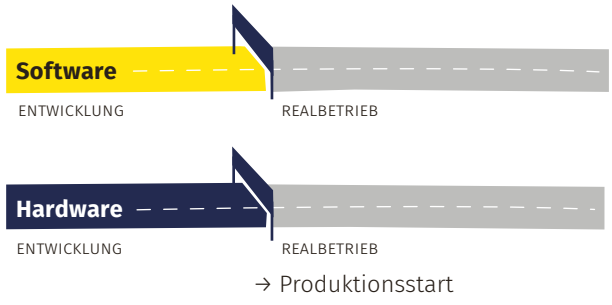
Im sogenannten Software-defined Vehicle (SDV) ist diese Kopplung aufgebrochen: Die Software wird auch nach dem Produktionsstart der Hardware kontinuierlich weiterentwickelt werden. Ähnlich wie bei Smartphones oder PCs können Funktionen jederzeit durch Software ergänzt oder verändert werden Hinzu kommt eine stärkere Vernetzung des Fahrzeugs und seine Einbindung in Software- und Serviceökosysteme. Das SDV kann so beispielsweise Sensor-Informationen mit anderen Fahrzeugen austauschen oder stark personalisiert werden, etwa indem Funktionen im SDV bedarfsorientiert und zeitlich begrenzt freigeschaltet werden.

Stellen Sie sich beispielsweise vor, Sie könnten für die Dauer eines Ski-Urlaubs spezialisierte Fahrassistenzsysteme freischalten, die das Fahren bei Schnee und Eis erheblich erleichtern, in Ihrem Alltag außerhalb des Urlaubs aber nicht benötigt werden. Zusätzlich könnte Ihnen Ihr SDV beispielsweise vorschlagen, temporär Software zur Kommunikation mit dem Verkehrsleitsystem des Urlaubsorts zu installieren.

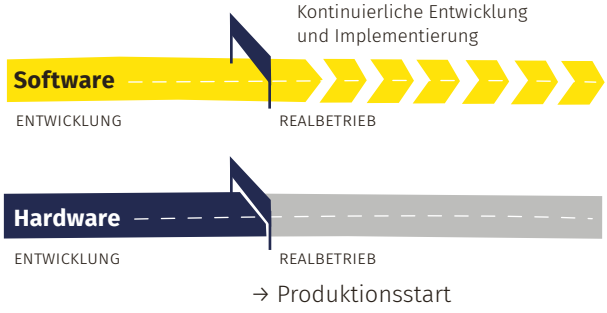
Gangwechsel

Das ist die Vision hinter dem Software-defined Vehicle: Nach dem Produktionsstart kann die Software, anders als die Hardware, weiterhin angepasst und optimiert werden.

Gestern: Hard- und Software gekoppelt



Morgen: Hard- und Software entkoppelt

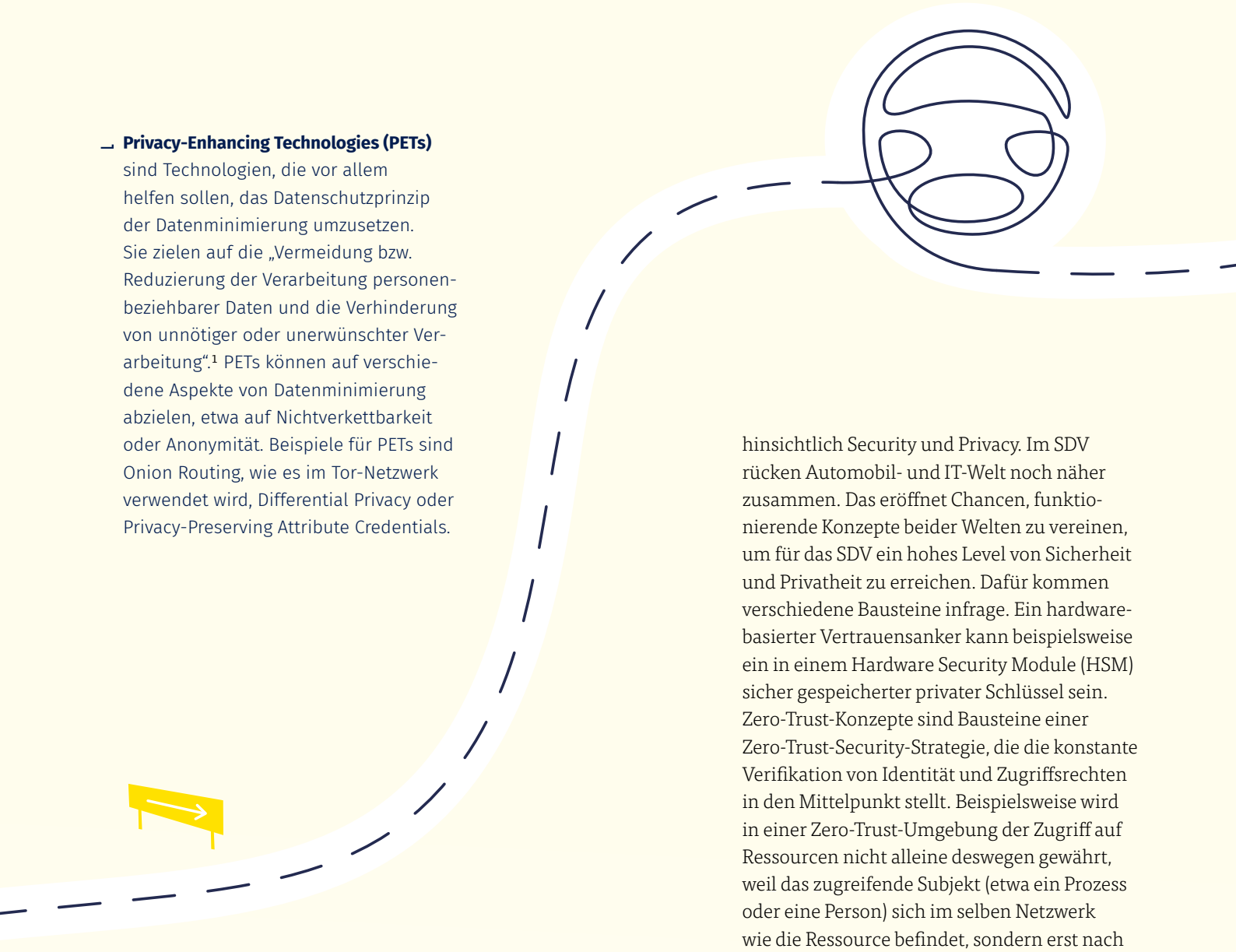


Safety meets Security

Was Sicherheit und Privatsphäre angeht, bringen höhere Vernetzung und wachsende Bedeutung von Software aber auch einige Herausforderungen mit sich. Verglichen mit anderen hochvernetzten Systemen, wie zum Beispiel Smartphones, müssen Fahrzeuge schließlich auch hohe Anforderungen an die Sicherheit im Sinne der „Safety", also der Betriebssicherheit, erfüllen. Maßnahmen zum Schutz der Sicherheit im Sinne von „Security" und „Privacy" müssen daher stets auch unter dem Aspekt ihres Einflusses auf die Safety betrachtet werden. Daher trifft die oft bemühte Metapher vom „Smartphone auf Rädern" letztlich auf Fahrzeuge nur bedingt zu.

Mit steigender Vernetzung und der zunehmenden Bedeutung von Software bieten sich natürlich auch neue Angriffsmöglichkeiten und -ziele. Am bedrohlichsten scheinen Angriffe, die es ermöglichen würden, aus der Ferne die Kontrolle über ein Fahrzeug zu übernehmen. Angriffe müssen aber nicht zwangsläufig das Fahrzeug selbst ins Visier nehmen. Auch Backendsysteme können angegriffen werden, etwa um die Privatsphäre der Person

Privacy-Enhancing Technologies (PETs) sind Technologien, die vor allem helfen sollen, das Datenschutzprinzip der Datenminimierung umzusetzen. Sie zielen auf die „Vermeidung bzw. Reduzierung der Verarbeitung personenbeziehbarer Daten und die Verhinderung von unnötiger oder unerwünschter Verarbeitung".[1] PETs können auf verschiedene Aspekte von Datenminimierung abzielen, etwa auf Nichtverkettbarkeit oder Anonymität. Beispiele für PETs sind Onion Routing, wie es im Tor-Netzwerk verwendet wird, Differential Privacy oder Privacy-Preserving Attribute Credentials.



zu verletzen, der das Fahrzeug gehört[2], oder massive Verkehrsbehinderungen auszulösen. Wie so etwas aussehen kann, zeigt eine Attacke auf einen russischen Taxivermittlungsdienst: Diese führte dazu, dass Dutzende Taxis an dieselbe Adresse gelotst wurden und so massive Verkehrsbehinderungen in Moskau auslösten.[3]

Das Beste aus beiden Welten

Mit der veränderten Fahrzeugarchitektur, der größeren Dynamik des Fahrzeugsystems und der stärkeren Einbindung des Fahrzeugs in größere, komplexe Mobilitäts(öko)systeme bieten sich aber auch neue Möglichkeiten hinsichtlich Security und Privacy. Im SDV rücken Automobil- und IT-Welt noch näher zusammen. Das eröffnet Chancen, funktionierende Konzepte beider Welten zu vereinen, um für das SDV ein hohes Level von Sicherheit und Privatheit zu erreichen. Dafür kommen verschiedene Bausteine infrage. Ein hardwarebasierter Vertrauensanker kann beispielsweise ein in einem Hardware Security Module (HSM) sicher gespeicherter privater Schlüssel sein. Zero-Trust-Konzepte sind Bausteine einer Zero-Trust-Security-Strategie, die die konstante Verifikation von Identität und Zugriffsrechten in den Mittelpunkt stellt. Beispielsweise wird in einer Zero-Trust-Umgebung der Zugriff auf Ressourcen nicht alleine deswegen gewährt, weil das zugreifende Subjekt (etwa ein Prozess oder eine Person) sich im selben Netzwerk wie die Ressource befindet, sondern erst nach expliziter Authentisierung und Prüfung der Berechtigungen des Subjekts. Einen anderen Baustein können Vehicle Security Operation Center darstellen, die der zentralen Überwachung der Sicherheit ganzer Fahrzeugflotten und der schnellen Reaktion auf erkannte Sicherheitsprobleme dienen. Dort laufen etwa Daten von fahrzeugseitigen Intrusion-Detection-Systemen zusammen. Sichere Virtualisierung auf eingebetteten Systemen ist notwendig, um verschiedene Applikationen im Fahrzeug wechselwirkungsfrei und sicher auf derselben Hardware ausführen zu können. Dies gewinnt im SDV an Relevanz, da

PETs im Check

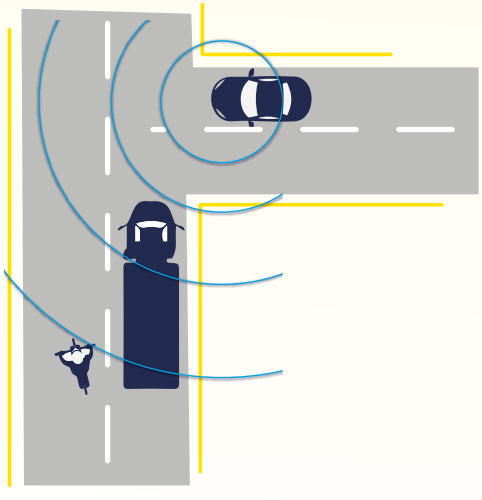
Privacy-Enhancing Technologies zielen vor allem auf Datenminimierung ab (siehe links). Wie sie im Kontext von SDVs funktionieren können, zeigen drei Szenarien.

Trusted Execution Environments (TEEs) schützen, basierend auf Hardware-Mechanismen, Daten und Programmcode üblicherweise durch deren Speicherung in verschlüsselten Speicherbereichen und die Einschränkung des Zugriffs auf diese Bereiche. Dadurch sind Daten und Code selbst im Falle der Kompromittierung des Betriebssystems geschützt. Im Kontext des SDV ist eine Vielzahl von Anwendungsfällen für TEEs inner- und außerhalb des Fahrzeugs denkbar – so zum Beispiel maschinelles Lernen mit schützenswerten Daten. Bosch Research hat gemeinsam mit Partnern ein Konzept vorgestellt[4], um Bildmaterial, das von Fahrzeugen mittels Frontkameras aufgenommen wurde, sicher für das Trainieren von Assistenzsystemen zu verwenden. Dabei werden die Bilder zunächst vom Fahrzeug verschlüsselt in ein Backend übertragen. Dort werden personenbeziehbare Elemente der Bilder, so zum Beispiel Gesichter, in einer TEE automatisch erkannt, aus dem Gesamtbild herausgeschnitten und verschlüsselt gespeichert. Erst im Moment des tatsächlichen Lernens werden die personenbeziehbaren Details und die restlichen Bildteile innerhalb einer TEE wieder zusammengesetzt, um ein statistisches Modell auf realistischen und unveränderten Daten zu trainieren. Die personenbeziehbaren Elemente bleiben dabei stets verschlüsselt bzw. in einer TEE vor Zugriff geschützt, um Risiken für die Betroffenen zu reduzieren.

Secure Multiparty Computation (MPC) sind Verfahren, die insbesondere dann von Vorteil sind, wenn Berechnungen auf sensiblen Daten mehrerer Parteien ausgeführt werden sollen und das Ergebnis (nicht aber die Inputdaten) allen an der Berechnung Beteiligten zugänglich gemacht werden soll. Vorstellbar sind hier etwa Analysen auf Daten unterschiedlicher Parteien wie Betreibern von Verkehrsleitsystemen, Fahrzeugherstellern oder Mobilitätsdienstleistern. Zwar ist MPC aktuell für viele Anwendungsfälle noch nicht leistungsstark genug, das Feld entwickelt sich momentan aber rapide weiter. Ein Beispiel dafür ist das mit dem dritten Platz beim Deutschen IT-Sicherheitspreis 2022 ausgezeichnete Open-Source-Projekt „Carbyne Stack“[5], das Cloud-Native-Technologien mit MPC zusammenführt.

Attribute-Based Credentials (ABCs) sind, vereinfacht ausgedrückt, Authentifizierungsmechanismen, die es erlauben, ausgewählte Eigenschaften nachzuweisen, ohne die entsprechenden Werte offenlegen zu müssen. So können ABCs zum Beispiel verwendet werden, um Volljährigkeit nachzuweisen, ohne das Geburtsjahr preiszugeben. Im Kontext des SDV haben sie das Potenzial, die Verwendung von Mobilitätssystemen, etwa im Platooning oder Carsharing, datensparsamer umzusetzen[6] oder Zugangskontrollen (etwa zu Umweltzonen oder Parkbereichen) datenschutzfreundlicher zu gestalten.

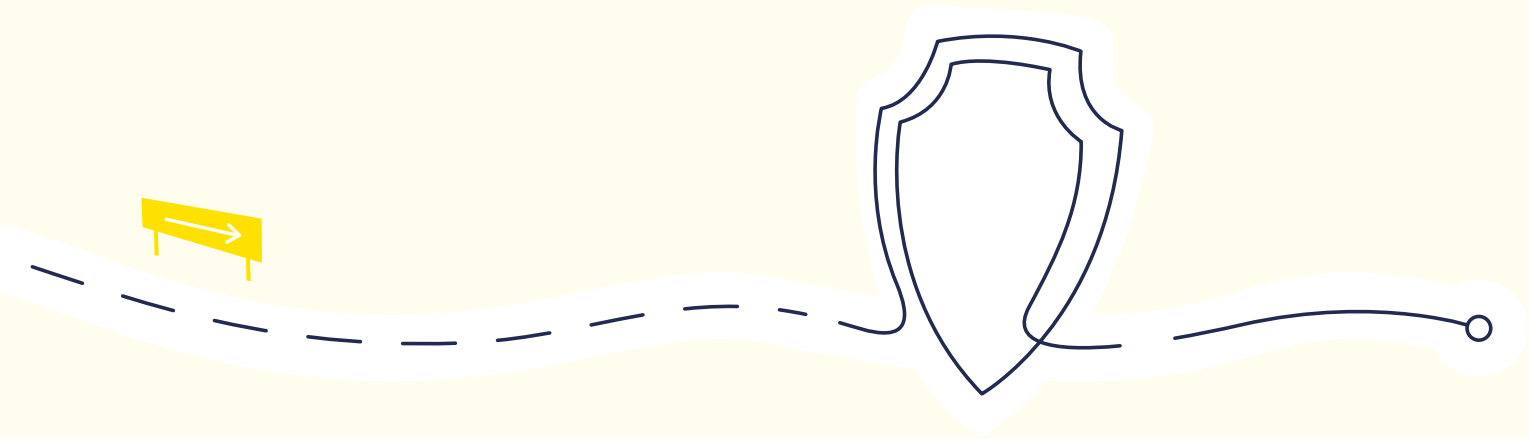
Applikationen dort zunehmend auf wenigen zentralen Fahrzeugcomputern statt getrennt in vielen spezialisierten Steuergeräten ausgeführt werden. Fest steht: Das SDV wird, mehr als herkömmliche Fahrzeuge, Daten sammeln und generieren, um erweiterte Funktionalität und Sicherheit zu bieten. Dies kann beispielsweise über Fahrzeugsensoren wie Frontkameras oder Innenraumsensoren erfolgen. Wertvolle Daten werden aber auch von anderen Fahrzeugkomponenten erzeugt, beispielsweise im Zuge des Batteriemanagements[7].



Durch Vernetzung von Fahrzeugen lassen sich auch Unfälle vermeiden. So können gefährliche Situationen frühzeitig angekündigt werden, etwa wenn sich ein Motorrad aus einer nicht gut einsehbaren Richtung nähert.

Des Weiteren wird das SDV vernetzte Funktionen und sogenannte V2X-Applikationen (vehicle-to-everything) nutzen, durch die Fahrzeuge mit ihrer direkten Umgebung in Kontakt stehen. Diese können die Verkehrssicherheit erhöhen, hinterlassen aber auch Datenspuren. Beispielsweise werden V2X-Warnnachrichten (etwa über liegen gebliebene Fahrzeuge oder Straßenglätte) als Broadcast-Nachrichten an andere Fahrzeuge gesendet. Dieser Datenaustausch kann viel Gutes bewirken, birgt aber auch Risiken, was die Privatsphäre der Fahrerinnen und Fahrer angeht. Bereits heute werden die bestehenden Security- und Datenschutzkonzepte daher konsequent weiterentwickelt, um auch für das SDV ein hohes Schutzniveau zu erreichen. Neben den oben genannten Bausteinen könnten in Zukunft auch die bisher noch vergleichsweise wenig verbreiteten Privacy-Enhancing Technologies (PETs) eine größere Rolle spielen. Für deren Potenzial gibt es viele Beispiele (siehe S.27).

Damit SDVs auf dem Markt und im Verkehr gut ankommen, dürfen sie in puncto Security und Privacy keine Mängel aufweisen. Das hat auch die Branche verstanden: Der Reifegrad von Security und Privacy Engineering in der Automobilindustrie ist in den vergangenen Jahrzehnten stark gestiegen. Mit dem Aufkommen des SDV ist es zudem zwingend notwendig, bestehende Mechanismen und Verfahren weiterzuentwickeln, um die neuen Herausforderungen zu meistern. Dass dabei IT- und Automobilwelt näher zusammenrücken, bietet



enorme Chancen. Und um diese zu nutzen, sind Privacy-Enhancing Technologies ein wichtiger Baustein. Sie haben das Potenzial, nicht nur ein Teil der Lösung der Security- und Privacy-Herausforderungen für die Mobilität der Zukunft zu sein, sondern auch neue, kollaborative und die Privatheit wahrende Datennutzungskonzepte zu ermöglichen. Sie können allerdings nur einen von vielen Bausteinen eines umfassenderen Konzepts darstellen. Dies liegt nicht nur an offenen technischen Herausforderungen, sondern auch daran, dass jegliche Umsetzung technischer Maßnahmen durch organisatorische Maßnahmen ergänzt werden und in ein umfassenderes Cybersecurity Management System integriert sein muss.

Die Fachgruppe PET
hat sich zum Ziel gesetzt, alle relevanten Aspekte zu Privacy-Enhancing Technologies und Datenschutzfördernder Technik in die aktuellen Diskussionen sowohl der Wissenschaft, Wirtschaft und Gesetzgebungsorgane als auch der Anwender*innen selbst und in Projekte des Fachbereichs Sicherheit der GI einzubringen und deren technologischen, gesellschaftlichen und wirtschaftlichen Nutzen im Kontext mit Themen der Informatik zu erklären.
fg-pet.gi.de

Deep Dive
Für alle, die tiefer in die Materie einsteigen wollen, gibt es zusätzliche Leseempfehlungen wie immer online: *inf.gi.de/SDV*

Über den Autor
Dr. Christian Zimmermann ist Fachreferent für Cybersecurity und Privacy bei der Robert Bosch GmbH. Sein Tätigkeitsgebiet dort ist die Technologiestrategie für Produkt-Cybersecurity im Bereich Bosch Mobility. Zuvor forschte er bei Bosch Research an Security- und Privacy-Technologien für unterschiedlichste Einsatzszenarien. Er erhielt sein Diplom in Wirtschaftsinformatik von der Universität Mannheim und promovierte an der Universität Freiburg. Er ist momentan Mitglied der Ad-Hoc Working Group on Data Protection Engineering der European Union Agency for Cybersecurity.

[1] Borking, John J. & Raab, Charles D. (2021), *"Laws, PETs and other technologies for privacy protection"*. In: Journal of Information, Law and Technology, übersetzt durch den Autor

[2] Siehe bspw. *https://samcurry.net/web-hackers-vs-the-auto-industry/*

[3] *https://www.spiegel.de/netzwelt/apps/russland-moskau-hacker-loesen-offenbar-mit-taxi-app-riesigen-stau-aus-a-08092b45-f3b2-49a6-9549-580dfaaa5806*

[4] Siehe auch *https://www.youtube.com/watch?v=UeipdWzsdUo*

[5] *https://carbynestack.io/*

[6] Siehe bspw. Zimmermann, Christian et al. (2019), *"Attribute-Based Credentials in High-Density Platooning"*

[7] Siehe auch *https://www.bosch-mobility.com/de/loesungen/software-und-services/battery-in-the-cloud/battery-in-the-cloud/*