Elektronische Manipulation von Fahrzeugen

Dr. Ingo Holtkötter
Ingenieurbüro Schimmelpfennig + Becke GmbH & Co. KG, Münster, Germany

Abstract
Due to the increasing importance of electronic systems in vehicles covering driving functions, entertainment systems and security devices, experts are asked questions related to electronic systems more frequently. The article gives an overview of the working areas which arise in the field of accident reconstruction and insurance fraud.
But with respect to insurance fraud in particular, the investigation of manipulation of electronic control units, e. g. changing odometer values, enabling additional functions or adding more keys to the car, is not widely known.

The work of car hackers on the one hand and security vulnerabilities of electronic vehicle systems on the other lead to a variety of successful hacking investigations resulting in odometer change, key cloning and car theft. To produce evidence for the court, it is essential for the expert to understand the manipulation technique and to be able to show and perform a corresponding manipulation oneself.

The basic investigation approaches and methods are shown with several examples such as changing the odometer, analyzing key fob signals or reading data from protected memory chips.

Zusammenfassung
Durch die zunehmende Ausstattung moderner Fahrzeuge mit Elektronik und die Verlagerung vieler Bedienfunktionen als Softwarebausteine, gewinnen Fragen zur Fahrzeugelektronik auch bei gerichtlichen Aufträgen immer mehr an Bedeutung. Der Artikel gibt einen Überblick über die Themenbereiche des unfallanalytischen Sachverständigen im Bereich der Fahrzeugelektronik.
Während das Auslesen von Fehlerspeichern und anderen Speichern im Rahmen der Verkehrsunfallrekonstruktion bereits vielfach an anderer Stelle beschrieben wurde, legt der vorliegende Artikel den Fokus auf den Versicherungsbetrug, insbesondere auf die Tachomanipulation, Veränderung von Steuergeräten und Schlüsselmanipulation.
Für eine fundierte Analyse, die gerichtlichen Standards entsprechen kann, ist es unbedingt erforderlich, dass sich der Sachverständige selbst das notwenige Wissen und die Fähigkeiten verschafft, entsprechende Manipulationen selbst analysieren und durchzuführen zu können.

Die prinzipielle Vorgehensweise für die Analyse derartiger Fragen wird anhand von Beispielen im Bereich der Tachomanipulation, der Schlüsselanalyse und Auslesen geschützter Bausteine gezeigt.

Einleitung

Während sich technische Manipulationen („Tuning“) von Fahrzeugen bis vor einigen Jahren auf den Umbau mechanischer Teile bezog, werden diese heutzutage durch Veränderung von Hardware- und Softwarekomponenten in den Steuergeräten vorgenommen. Da mittlerweile auch die modernen Fahrzeuge im unteren Preissegment mit immer mehr Fahrzeugelektronik ausgestattet werden, sind in der Praxis elektronisch manipulierte Fahrzeuge in allen Fahrzeugklassen zu finden. Dabei geht es nicht nur um Tuningmaßnahmen wie Leistungssteigerung oder Veränderung der Motorcharakteristik, sondern auch um die Veränderung der fahrzeugspezifischen Daten.

Typische Manipulationen sind das Zurückstellen des Kilometerstands, das Überwinden von Diebstahlwarnanlagen und das Kopieren von Schlüsseln. Zunehmend ergeben sich auch Fragen zu Elektronik- und Softwareproblemen als Wandlungsgrund zum Rücktritt eines Kaufvertrages.[1]

Der vorliegende Artikel gibt eine Übersicht zur elektronischen Manipulation von Fahrzeugen in den Bereichen Tachomanipulation, Manipulation und Kopieren von Schlüsseln bzw. Zugangssystemen sowie die Veränderung oder das Auslesen von Steuergeräten.
Das hier dargestellte Auslesen der Steuergeräte erfolgt durch direkten Zugriff auf die Speicherbausteine, d.h. sowohl der Aufwand als auch der Erkenntnisgewinn geht weit über die Möglichkeiten der normalen Fahrzeugdiagnose hinaus.

Durch den Autor wurden im Rahmen von gerichtlichen Gutachten bereits einige derartige Untersuchungen durchgeführt und es stellt sich die Frage, wie mit den gewonnenen Informationen umgegangen werden darf und welche juristischen Probleme sich bei der Zusammenarbeit von Sachverständigen untereinander ergeben können.

Es ist dabei sicher nicht unproblematisch, die mühsam gewonnenen Erkenntnisse detailliert im Gutachten zu beschreiben oder gar zu veröffentlichen. Zum Abschluss des Artikels werden daher die juristischen Grenzen, die sich für den technischen Sachverständigen nach aktuellem Kenntnisstand zumindest in Deutschland ergeben, angesprochen und zur Diskussion gestellt.

Manipulation von Tachometern und Freischalten von Funktionen

Ein klassisches Beispiel der Manipulation von Fahrzeugen ist die Veränderung des Gesamtkilometerstands in der Tachoeinheit. Für die Beantwortung der typischen Beweisfragen zum Aufwand und zum Nachweis einer möglichen Manipulation ist es notwendig, dass sich der Sachverständige selbst das nötige Wissen und die Fähigkeiten verschafft. Nur dann kann eine fundierte technische Analyse erfolgen.[2,3]

Ein sinnvoller Ausgangspunkt einer derartigen Untersuchung besteht im Studium der technischen Unterlagen des Fahrzeugs (zum Beispiel über die Online-Portale der Hersteller[4]). Meist lässt sich den technischen Angaben entnehmen, welche Steuergeräte für die Kontrolle und die Anzeige des Tachostands verantwortlich sind.

Abb. 1: Untersuchung der Datenprotokolle in einer Tachoeinheit (Mercedes Benz W163) und "Korrektur" der Laufleistung von 280.134 km auf 93.248 km

Im Rahmen eines gerichtlichen Gutachtens wurde bspw. durch den Autor zunächst die Elektronik einer Tachoeinheit zerlegt und der Speicherbaustein für den Kilometerstand identifiziert (siehe Abb. 1, oben).
In einfachen Fällen ist es ausreichend, die auf den Bauteilen aufgedruckten Bezeichnungen zu recherchieren, da meist nur ein Speicherbaustein verbaut ist. Nach der Analyse des Datenprotokolls zum Speicherchip mit den entsprechenden Geräten (Oszilloskop, Logik-Analyzer, Protokoll-Analyzer) und des gespeicherten Datenformats konnte dann der angezeigte Tachostand verändert werden (siehe Abb.1, unten). Das Kombiinstrument kann danach wieder in das Fahrzeug eingesetzt und verwendet werden. Damit konnte die Frage zur Durchführbarkeit einer derartigen Manipulation zweifelsfrei beantwortet werden.

Modernere Kombiinstrumente lassen sich auch über die Diagnoseschnittstelle umprogrammieren, so dass ein Ausbau nicht mehr notwendig ist. Abb. 2 zeigt exemplarisch den Einsatz zweier – in Deutschland illegaler – Programmiergeräte.

Abb. 2: Verwendung von Tachoprogrammiergeräten

Ein Beispiel einer konkreten Tachoveränderung mit einem solchen Gerät ist in Abb. 3 dokumentiert.

Eine Manipulation des Kilometerstands ist in vielen Fällen nachweisbar, weil es häufig noch andere Steuergeräte in den Fahrzeugen gibt, die die aktuelle Laufleistung speichern und im

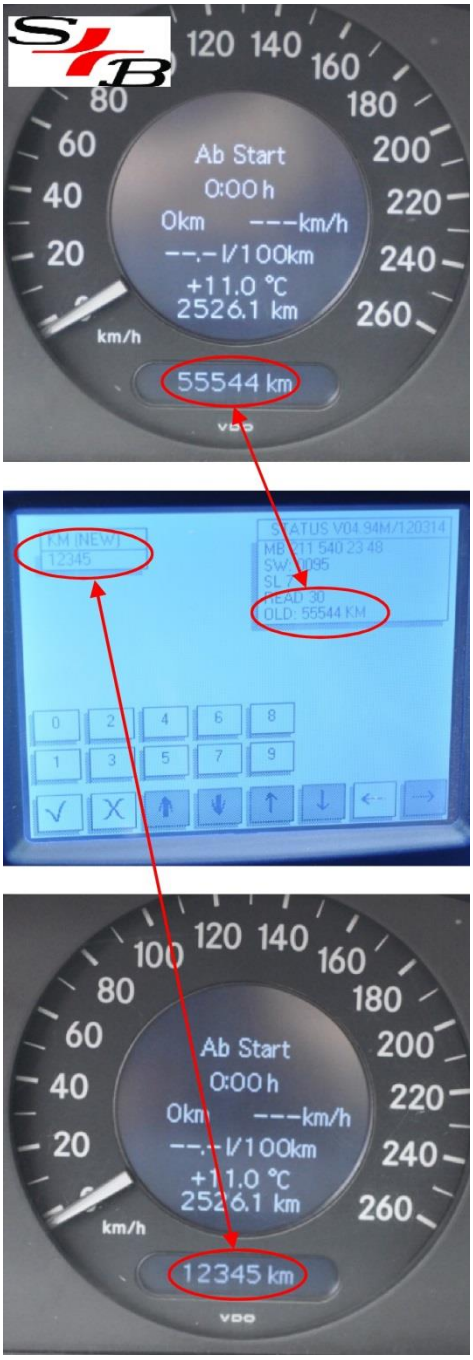


Abb 3: "Korrektur" der Laufleistung von 55.544 km auf 12.345 km an einer Mercedes-Benz E-Klasse (W211)

Betrieb untereinander austauschen, bzw. sich gegenseitig kontrollieren. Insbesondere bei modernen Fahrzeugen ist dadurch der Aufwand einer Tachomanipulation sehr hoch.

Falls das Fahrzeug über Telematik-Dienste verfügt (bspw. Mercedes Me Connect, BMW Connected Drive, Jaguar In Control etc.), ist eine „perfekte" Manipulation des Tachostands kaum noch möglich, da mit Hilfe der beim Fahrzeughersteller, auf den Internet-Servern des Portalbetreibers, in den Werkstätten und ggfs. sogar den Mobiltelefonen der Fahrzeughalter gespeicherten Daten eine derartige Manipulation schnell aufzudecken ist. Da aber nur wenige Fahrzeuge bisher mit solchen Funktionen ausgestattet sind, wird der Gebrauchtmarkt von Fahrzeugen aber sicher noch viele Jahre mit manipulierten Fahrzeugen übersäht sein.

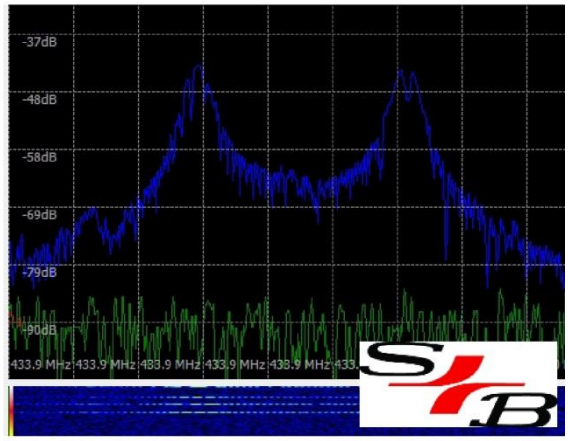
Manipulation von Schlüsseln und Zugangssystemen

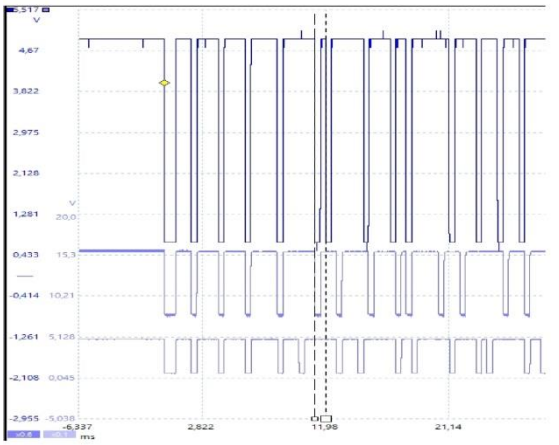
Eine weitere naheliegende Manipulation umfasst das Öffnen und den Diebstahl von Fahrzeugen bzw. das Anlernen neuer Schlüssel.[5,6] Zunächst bietet es sich auch hier an, in den Service-Portalen der Hersteller zu recherchieren, welches Schlüsselsystem eingesetzt wird und welche Steuergeräte in die Wegfahrsperrenfunktion involviert sind.

Bei Fahrzeugschlüsseln wird unterschieden zwischen der Zugangsberechtigung (Öffnen des Fahrzeugs) und der Fahrberechtigung (Starten und Fahren des Fahrzeugs). Zum Öffnen des Fahrzeugs kann die Funkfernbedienung des Schlüssels oder der Schließmechanismus am Fahrzeug als Angriffsfläche dienen. Grundlagen zur Funktion von Fahrzeugschlüsseln wurden durch den Autor bereits an anderer Stelle zusammengefasst.[7,8]

Das Entschlüsseln des Fernbedienungscodes ist bei einigen Fahrzeugen bereits erfolgreich durchgeführt worden und ermöglicht damit einem Angreifer den freien Zugang zum Fahrzeug, indem die Zentralverriegelung per Funk geöffnet wird.[9,10]
Die Abb. 4 zeigt eine Analyse der Funkfernbedienung eines Oberklasse-fahrzeugs, die durch den Autor in Rahmen eines Gerichtsgutachtens durchgeführt wurde. Im oberen Bild ist das Frequenzspektrum des

Funksignals gezeigt, das mittlere Bild zeigt das übertragene Signal (d.h. die Information, die hier in den verschiedenen Pulslängen codiert ist).





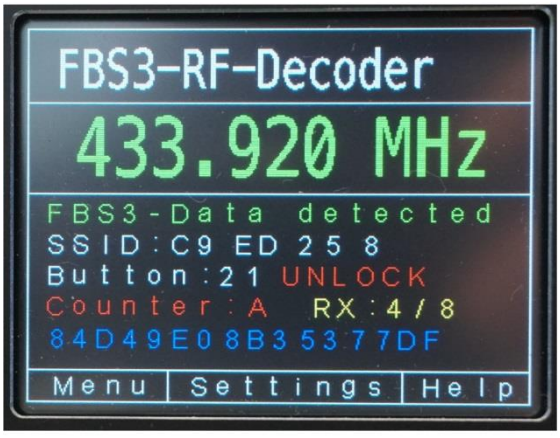


Abb. 4: Analyse eines Schlüssel-Funksignals: oben: Frequenzspektrum, Mitte: codierte Nachricht, unten: decodierte Nachricht

Im unteren Bild ist mit Hilfe eines selbstgebauten Decoders die entschlüsselte Nachricht dokumentiert. So lässt sich z.B. ablesen, zu welchem Schlüsselsatz und damit zu welchem individuellen Fahrzeug der Schlüssel gehört und welche Taste gedrückt wurde.
Im gezeigten Beispiel wurde ein Funksignal eines Mercedes-Schlüssels des Schlüsselsatzes C9 ED 25 8 mit der Taste zum Entriegeln (UNLOCK) empfangen.

Nachdem das Funksignal decodiert und bekannt ist, muss in der Regel auch das Schließsystem des Fahrzeugs untersucht werden, um Möglichkeiten zum Diebstahl oder Anlernen neuer Schlüssel zu analysieren. Hierzu werden die Signale auf den CAN-Systemen der Fahrzeuge mitgelesen sowie die gespeicherten Daten in den Steuergeräten untersucht. Ein einfacher Ansatz besteht z. B. darin, die oben beschriebene Information des Funksignals in den CAN-Bus-Daten zu suchen. Wenn bekannt ist, wie diese Information über den CAN-Bus übertragen wird, kann ggfs. auch geprüft werden, wie das Fahrzeug auf andere Schlüsseldaten reagiert.

Öffnen und Auslesen von Steuergeräten

Während das mechanische Öffnen eines Steuergerätes meist leicht und intuitiv möglich ist, ist der Zugriff auf die z.T. gegen Auslesen geschützten Speicherbausteine eine Spezialaufgabe. Nachdem man herausgefunden hat, welcher Prozessor zum Einsatz kommt, kann dann mit Hilfe spezieller Werkzeuge auf die Geräte zugegriffen werden. Oft hilft auch das Diagnosesystem der Hersteller, mit dem zum Teil das Auslesen besonderer Daten erfolgen kann.

Abb. 5 zeigt das Auslöten eines Airbagmodul-Prozessors (links) und den Anschluss eines elektronischen Zündschlosses an ein spezielles

Programmiergerät (rechts), das die Kommunikation trotz Auslesesperre ermöglicht. Mit solchen Daten können z.B. Airbagsteuergeräte nach einem Crashereignis wiederverwendet oder deren Verhalten systematisch untersucht werden. Das Auslesen sensibler Prozessoren wie die der Steuergeräte zur Wegfahrsperre ist ein zentraler Bestandteil für die Analyse der Funktionsweise des Systems. Mit dem ausgelesenen Programmcode können beispielsweise die Schlüssel-Identifikationsdaten zum Programmieren neuer Schlüssel gewonnen werden. Oft kann der Programmcode nicht nur gelesen, sondern auch geschrieben werden, so dass es möglich wird, den Programmcode zu verändern und bspw. gezielt neue Schlüssel hinzuzufügen.

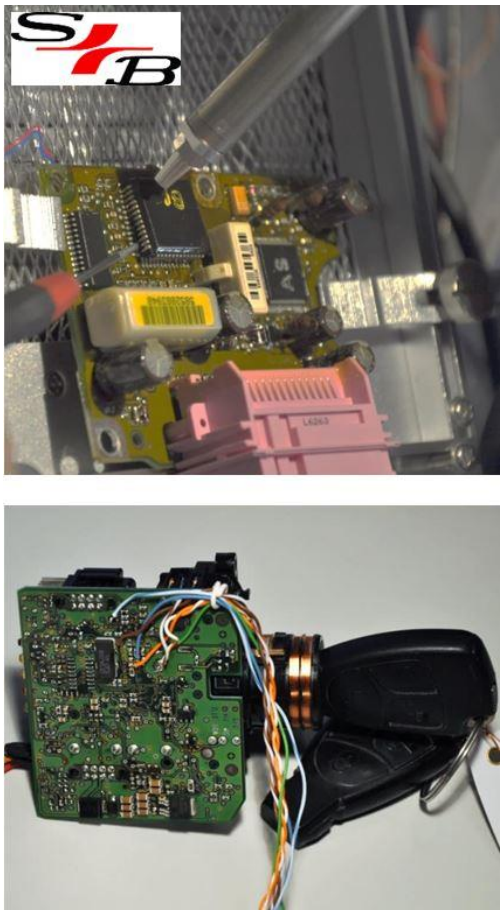


Abb. 5: Auslöten und Auslesen geschützter Prozessoren

Herausforderungen für den Sachverständigen und der Ausarbeitung gerichtlicher Gutachten

Im Allgemeinen ist es äußerst schwierig, belastbare Informationen zu derartigen Manipulationen zu finden. Um die gerichtlich gestellten Beweisfragen sicher beantworten zu können, ist es unerlässlich, dass sich der Sachverständige selbst das nötige Wissen verschafft und diese Manipulation auch selbst durch- und ggfs. vorführen kann.
Es darf nicht sein, dass ein Rechtsstreit auf Basis von Zeitschrifteninformationen oder gar Beiträgen aus dem Internet entschieden wird, ohne dass der Sachverständige selbst in der Lage ist, im Internet aufgestellte Behauptungen und Werbeaussagen zu überprüfen und zu beurteilen.

Für entsprechende Untersuchungen im Rahmen von Gerichtsverfahren müssen Sicherheits- und Verschlüsselungsmechanismen der Fahrzeughersteller umgangen und verdeckte elektronische Zugriffsmöglichkeiten aufwendig untersucht werden.

Es ist sicher nicht im allgemeinen Interesse, dass das technische Gutachten eines öffentlichen Prozesses eine detaillierte und bebilderte Anleitung zum Diebstahl eines Fahrzeugs enthält. Dabei ist sicherzustellen, dass die erlangten Informationen zur gezielten technischen Manipulation von Tachoständen oder dem Diebstahl von Fahrzeugen nicht in die falschen Hände gelangen.

Es ist natürlich andererseits naiv zu glauben, dass die entsprechenden Tätergruppen noch nicht über derartiges „Know-How“ verfügen. Eine ausführliche Darstellung dieser Thematik findet sich zusammen mit einer juristischen Bewertung in einem aktuellen Artikel der Neuen Zeitschrift für Verkehrsrecht (NZV).[11]

References

[1] I. HOLTKÖTTER: Elektronik- und Softwareprobleme als Wandlungsgrund?, Vortrag 7. Gerichtsseminar Unfallrekonstruktion, crashtest-service.com (13.04.2018)

[2] I. HOLTKÖTTER: Elektronische Manipulation von Fahrzeugen, Schwerpunkt Tachometer und Betriebsstundenzähler, Vortrag 74. Fachtagung Münchner Arbeitskreis für Straßenfahrzeuge e.V. (25.03.2017)

[3] T. GUT, M. KUGELE: Manipulation von Wegstreckenzählern – Untersuchungsmöglichkeiten für Sachverständige, Verkehrsunfall und Fahrzeugtechnik 07-08/2008, S. 210ff

[4] S. HEIDRICH, H. KIEBACH: Zugang zu Reparatur- und Wartungsinformationen, Verkehrsunfall und Fahrzeugtechnik 04/2014, S. 201ff

[5] M. GÖTH: Der Kraftfahrzeugdiebstahl in der Praxis – Teil 1, Verkehrsunfall und Fahrzeugtechnik 01/2009, S. 21ff

[6] M. GÖTH: Der Kraftfahrzeugdiebstahl in der Praxis – Teil 2, Verkehrsunfall und Fahrzeugtechnik 01/2009, S. 63ff

[7] I. HOLTKÖTTER: Elektronische Fahrzeugschlüssel als Sicherheitsproblem? Teil 1 – Grundlagen, Verkehrs-Rechts-Report (VRR) 07/2010, S.258ff

[8] I. HOLTKÖTTER: Elektronische Fahrzeugschlüssel als Sicherheitsproblem? Teil 2 – Manipulationsmöglichkeiten, Verkehrs-Rechts-Report (VRR) 08/2010, S. 296ff

[9] F. GARCIA, D. OSWALD, T. KASPER, P. Pavlidès: Lock It and Still Lose It – On the (In)Security of Automotive Remote Keyless Entry Systems, 25th USENIX Security Symposium

[10] R. VERDULT, F. GARCIA, B. Ege: Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer, 22nd USENIX Security Symposium

[11] I. HOLTKÖTTER, M. NUGEL: Die Aufklärung elektronischer Manipulationen von Fahrzeugen im Spannungsfeld zu Betriebsgeheimnissen der Hersteller, Neue Zeitschrift für Verkehrsrecht 05/2018, S. 128ff

Contact

Schimmelpfennig + Becke GmbH & Co. KG
Dr. rer. nat. Ingo Holtkötter
Münsterstraße 101
48155 Münster, Germany
e-mail: holtkoetter@ureko.de
Tel: +49 2506 820-0