Elektronische Fahrzeugschlüssel als Sicherheitsproblem?

Teil 2 – Manipulationsmöglichkeiten

*von Dr. Ingo Holtkötter, Münster**

Fortsetzung aus VRR 2010, 258 ff.

Im ersten Teil dieses Artikels wurden die technischen Grundlagen und die Funktionsweise verschiedener Fahrzeug-Fernbedienungen und Schlüssel dargestellt. Sowohl für die Datenübertragung vom Schlüssel zum Fahrzeug als auch für die Codierung der Daten werden je nach Fahrzeugtyp verschiedene Verfahren eingesetzt. Im vorliegenden zweiten Teil werden Manipulationsmöglichkeiten und Sicherheitsrisiken beschrieben, die generell einen Fahrzeugdiebstahl durch elektronische Manipulation nicht mehr unmöglich erscheinen lassen. Hierbei gilt es jedoch zu beachten, dass bei der Beurteilung eines Diebstahlrisikos die Technik des spezifischen Fahrzeugtyps von entscheidender Bedeutung ist, da unterschiedliche Steuergerätevarianten wiederum völlig andere Verhalten zeigen können.

I. Manipulationsmöglichkeiten der Funk- bzw. IR-Fernbedienung

1. Verhinderung des Schließvorgangs durch eine externe Funkstörung

Das Funksignal einer Fahrzeugfernbedienung wird bei europäischen Fahrzeugmodellen mit wenigen Ausnahmen mit einer Frequenz von etwa 433 MHz übermittelt. Wenn gleichzeitig ein starker Sender derselben Frequenz in der Umgebung aktiv ist, kann dies dazu führen, dass der Empfänger im Fahrzeug das relativ schwache Signal des Schlüssels nicht mehr erkennen kann. Dies ist vergleichbar mit einem Flüstergespräch während jemand im nebenstehenden Fahrzeug die Hupe betätigt. Wird das leise Gespräch von der sehr lauten Hupe übertönt, sind die gesprochenen Wörter nicht mehr zu verstehen. Diese Schwachstelle ist seit einigen Jahren bekannt und gerade deshalb so kritisch, weil man entgegen vielen Darstellungen in den Medien dazu nicht zwangsweise eine spezielle Elektronik oder ein umgebautes Funkgerät verwenden muss, sondern auch für jedermann frei erhältliche **LPD-Funkgeräte** in der Lage sind, den Funkbefehl der Fernbedienung zu überdecken. Dies wurde an zahlreichen Fahrzeugen verschiedener Hersteller getestet. In Abb. 1 ist dargestellt, wie der gleichzeitige Einsatz der Funkgerät-Sendefunktion dazu führt, dass das **Fahrzeug nicht mehr auf die Fernbedienung** reagiert.

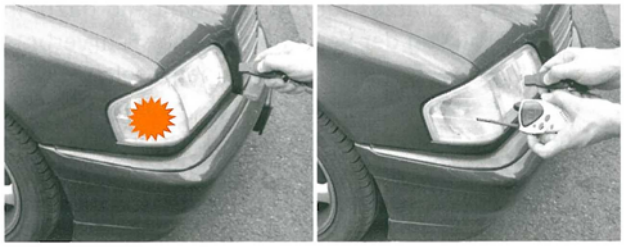

Abb. 1: Schließvorgang lässt sich durch ein geeignetes Funkgerät verhindern; links wird das Funksignal durch Blinken quittiert

In Abb. 2 wird der technische Hintergrund anhand der verschiedenen Funkspektren von Schlüssel und Funkgerät dargestellt. Im linken Bild ist das Frequenzspektrum um 433 MHz ohne Sendesignal dargestellt, es ist lediglich Hintergrundrauschen ohne Signalpeak in der Mitte des Spektrums zu erkennen. Das Spektrum im mittleren Bild zeigt das Funksignal eines VW-Schlüssels, welcher seine Codierung mit 433,92 MHz sendet, sobald der Knopf gedrückt wird. Im rechten Bild ist das Signal des Funkgerätes zu sehen, welches auf den entsprechenden Kanal für 433,92 MHz eingestellt wurde. Der Peak in der Mitte ist hier deutlich höher und damit auch stärker als der des Funkschlüssels. Durch Vergleich der gemessenen Funkspektren ist zu erkennen, dass das **Sendesignal des Funkgerätes das Schlüsselsignal überdecken kann**.

Ein Fahrzeugdieb kann bspw. auf einem großen Supermarktparkplatz mit seinem Funkgerät im passenden Moment dafür sorgen, dass ein Fahrzeug in der Nähe nicht verschlossen werden kann. Falls nun der Fahrer nicht genau darauf achtet, ob sein Fahrzeug den Befehl zum Verriegeln der Türen durch **Blinken quittiert**, bleibt das Fahrzeug trotz Knopfdruck auf der Fernbedienung offen. Wenn sich der Fahrer dann von seinem Fahrzeug entfernt, um in den Supermarkt zu gehen, kann der Fahrzeugdieb die unverschlossenen Fahrzeugtüren öffnen und dabei Gegenstände entwenden oder die Fahrzeugelektronik für einen späteren Diebstahl manipulieren.

Die Probleme, die im Zusammenhang mit den sog. LPD-Funkgeräten und **Fahrzeugschlüsseln, Garagentorantrieben sowie anderen Fernbedienungen** entstehen, haben dazu geführt, dass diese Art von Funkgeräten nur noch bis Ende 2013 für Sprach- und Datenübertragungen benutzt werden dürfen.

* Der Autor ist Sachverständiger für Straßenverkehrsunfälle sowie Unfälle mit mechanisch-technischem Gerät im Ingenieurbüro Schimmelpfennig + Becke, Münster.

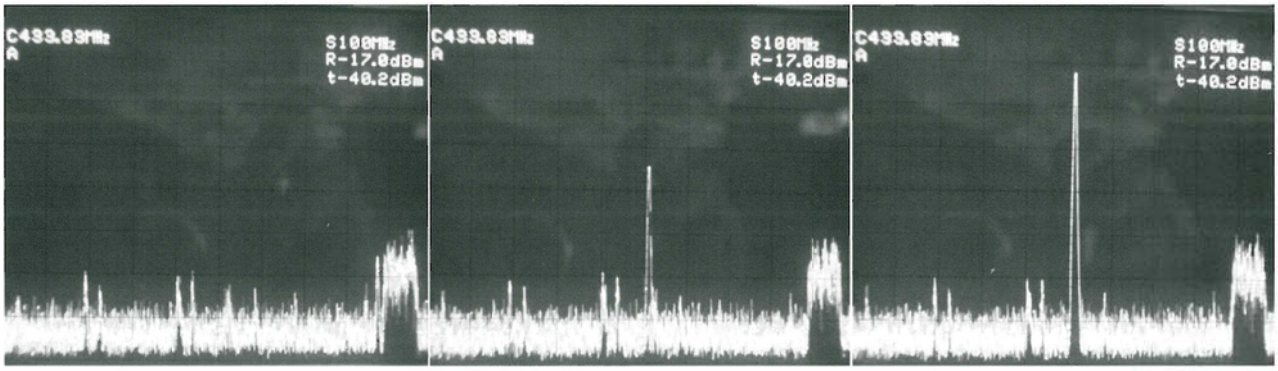

Abb. 2: Funksignalspektrum: links ohne Signal (Untergrundrauschen), Mitte VW-Schlüsselsignal und rechts das deutlich stärkere Sendesignal des Funkgerätes

2. Kopieren des Funksignals

Durch die unidirektionale Kommunikation vom Schlüssel zum Fahrzeug ist es möglich, den vom Schlüssel gesendeten Code einmalig mit einem entsprechenden Gerät aufzuzeichnen und später in der Nähe des Fahrzeugs wieder auszusenden. Auf diese Weise kann **jeder Funk- oder Infrarot-Schlüssel kopiert werden**. Hierbei ist allerdings zu beachten, dass bei Fahrzeugen mit Wechselcode der abgefangene Code nur einmalig gültig ist und das auch nur solange, bis der Schlüssel selbst wieder benutzt wird. Durch das **Wechselcodeverfahren** wird jeder ältere Code ungültig, sobald das Fahrzeug wieder einen neuen Code vom Schlüssel erhalten hat (s. hierzu auch den ersten Teil dieses Artikels in VRR 2010, 258 ff.).

Die Kopie des Funksignals ermöglicht auf diese Weise zwar einen Zugriff auf das Fahrzeug, ist aber durch den notwendigen zeitnahen und direkten Zugriff auf den Schlüssel nur begrenzt praktikabel. Denn wenn der Schlüssel für den Dieb zugänglich ist, kann er diesen auch direkt entwenden oder austauschen und damit das Fahrzeug öffnen und entwenden.

Dennoch ist so ein Angriff prinzipiell möglich und bei älteren **Fahrzeugen mit Festcodesender sowie vielen Garagentorantrieben erfolgreich**, weil bei diesen der abgespeicherte Code immer gültig bleibt und **jederzeit verwendet werden kann**.

3. Austesten aller möglichen Funkcodes

Durch die begrenzte Codelänge, die vom Schlüssel zum Fahrzeug übertragen wird, ist es denkbar, alle möglichen Codes auszutesten und abzuwarten, bis sich das Fahrzeug öffnet. Allerdings sind die Zugangssysteme so gestaltet, dass dafür ein **erheblicher Zeitaufwand** nötig ist. Bspw. wird bei BMW ein insgesamt 64bit langer Code gesendet, der im schnellsten Fall alle 30 ms wiederholt werden kann. Daraus ergibt sich eine Gesamtzeit von 17,5 Mrd. Jahre, die im Extremfall benötigt wird, um alle möglichen Codes auszuprobieren. Meist kann jedoch durch die Datenstruktur ein Teil der Daten bestimmt werden, sodass nicht alle Daten geraten werden müssen. Beim BMW-System resultieren daraus zwar nur noch etwa 32 unbekannte Bits, wofür jedoch immer noch ein Zeitaufwand von mehr als 4 Jahren Dauertesten benötigt würde. Insgesamt ist demnach eine sog. Brute-Force-Attacke im Allgemeinen **nicht zu erwarten**.

4. Manipulation der Fahrzeugelektrik

Prinzipiell ist es möglich, durch Tausch oder Manipulation an den entsprechenden Steuergeräten im Fahrzeug die **Wegfahrsperre** zu umgehen oder zu deaktivieren.

Wenn das Fahrzeug über die beschriebenen Methoden oder auch mechanisch geöffnet werden konnte, etwa über das mechanische Türschloss oder durch Einschlagen einer Scheibe, ist es auch möglich, zentrale **Steuergeräte auszutauschen** und dann mit dem Fahrzeug wegzufahren. Diese Variante ist sehr stark vom Fahrzeugtyp und der schnellen Austauschbarkeit der entsprechenden Steuergeräte abhängig. Passende Steuergerät-Schlüssel-Kombinationen könnten hierzu bspw. aus **Unfallfahrzeugen** entnommen werden. Wie auch die anderen vorgestellten Methoden setzt dies einen geplanten Diebstahl mit **umfangreicher Sachkenntnis sowie spezielle Vorbereitung** voraus.

Eine weitere Möglichkeit ist das **Zwischenspeichern von Schlüsselcodes** mit einem kleinen zusätzlichen Modul. In nahezu allen aktuellen Fahrzeugen wird der vom Schlüssel empfangene Code entweder über den Kabelbaum oder zumindest innerhalb eines Steuergerätes im **Klartext** übertragen. An dieser Stelle könnte ein zusätzliches Modul z.B. die letzten zehn Schlüsselcodes zwischenspeichern und erst dann weiterreichen. Wenn nach zehn gültigen Codes dann der elfte empfangen wird, wird der erste passende Code aus der Liste an die Fahrzeugelektronik weitergereicht und die gewünschte Funktion ausgeführt. Zwar setzt dies voraus, dass zeitweise eine zusätzliche Betätigung der Fernbedienung notwendig ist, in der Praxis wird sich jedoch kaum jemand wundern, wenn er mal zweimal die Fernbedienung bedienen muss. Auf diese Weise ist das Modul der Fahrzeugelektronik immer ein paar Codes voraus. Wenn nun auch noch unterschieden werden kann, ob ein Code zum Öffnen oder zum Schließen des Fahrzeugs gilt, kann das Modul dafür sorgen, dass man immer gülti-

ge Codes „in Reserve" hat, die über eine zusätzliche Fernbedienung dem Fahrzeugdieb die Zentralverriegelung aufsperren können. Bspw. ist denkbar, dass in der **Werkstatt** oder sogar bei einer **Probefahrt** ein zusätzliches Modul im Auto eingesetzt wird, wobei der Zeitaufwand hierfür etwa 1 – 2 Minuten beträgt. Daraufhin könnte Monate später das Auto entwendet werden. Ein solches Modul ist auch für ambitionierte Hobbybastler zu realisieren.

II. Manipulationsmöglichkeiten der Wegfahrsperre

1. Kopieren und Emulieren des Transponders

Der Transponder in den Fahrzeugschlüsseln, der über eine Sende-/Empfangsspule in der Zündschlosseinheit ausgelesen und beschrieben wird, konnte in den ersten Generationen der Wegfahrsperren (Anfang der 1990er Jahre) einfach kopiert werden. Die Transponder hatten zunächst nur eine **eindeutige Seriennummer**, die mit einem geeigneten Lesegerät ausgelesen werden kann. Später kamen zwar Transponder mit integriertem Speicher zum Einsatz, diese können jedoch im **Klartext ohne Verschlüsselung** ebenfalls ausgelesen werden. Falls das Fahrzeug nur einen Transponder mit einer bekannten Seriennummer akzeptiert, ist ein Angriff auch über eine elektronische Schaltung möglich, die einen Transponder **emuliert**. Diese hat den Vorteil, dass per Software **jede beliebige Seriennummer** vorgetäuscht werden kann. Auch in solchen Fällen ist es also möglich, den Transponder eines Schlüssels auszulesen und dann mit einer elektronischen Schaltung eine Kopie des Transponders herzustellen, mit der sich das Fahrzeug starten lässt. Die für das Kopieren notwendigen **Lese-/Schreibgeräte** sind wiederum von einem Hobbybastler bei entsprechender Fachkenntnis selbst herstellbar.

Bei einigen aktuellen Transpondersystemen ist ein solcher Angriff nicht mehr ohne Weiteres möglich, da die **Kommunikation zum Transponder verschlüsselt** erfolgt. Zur Überprüfung der Authentizität eines Schlüssels wird das sog. Challenge-Response-Verfahren eingesetzt. Hierbei wird vom Fahrzeug eine Aufgabe (Challenge) an den Transponder gesendet, die dieser mit seinem **geheimen Algorithmus** umrechnet und seine Antwort (Response) wieder an das Fahrzeug übermittelt. Nur wenn diese Antwort richtig ist, wird der Schlüssel erkannt. Für einen Fremden ist es nicht ohne Weiteres möglich, durch Abhören dieser Kommunikation den geheimen Algorithmus zu erraten.

Bei dem im letzten Artikel beschriebenen optischen Übertragungssystem bei Mercedes-Benz-Schlüsseln wird ebenfalls das Challenge-Response-Verfahren angewandt: Beim Einstecken des Schlüssels in die Zündschlosseinheit wird dieser über eine Spule mit Energie versorgt und sendet seine feste Kennung an das Zündschloss. Wenn die Schlüsselkennung dem Fahrzeug bekannt ist, antwortet die Zündschlosseinheit mit einer Aufgabe, die der Schlüssel umzurechnen hat. Diese Aufgabe wird bei jedem Anmeldeversuch verändert. Erst wenn der Schlüssel das jeweils richtige Ergebnis zurücksendet, wird die Lenkradsperre entriegelt. Nach diesem Vorgang prüft das Zündschloss in regelmäßigen Abständen, ob der Schlüssel noch im Zündschloss steckt. Wenn ein neuer Schlüssel angelernt werden soll, wird dieser vom Hersteller speziell auf das Fahrzeug vorcodiert und muss dann auch noch an das Fahrzeug angelernt werden.

2. Ausnutzung von Hersteller-Fehlern oder unzureichender Sicherheit

Ohne direkten Zugriff auf den Schlüssel ist eine Manipulation oder ein Vortäuschen eines echten Schlüssels möglich, falls die Implementierung der Codeübermittlung und Codebrechung **Fehler durch den Hersteller** aufweist. Einige Fahrzeughersteller benutzen bspw. das sog. KeeLoq-Verfahren, welches seit 2007 als überwindbar gilt. Einem **internationalen Forscherteam** der Universitäten Bochum und Teheran ist es gelungen, durch genügend langes Abfragen des Schlüssels ausreichend Information zu gewinnen, den geheimen Algorithmus des einen Schlüssels berechnen zu können. Hierzu ist ein **Funkkontakt zum Schlüssel für etwa 60 Minuten** und ein anschließendes Rechnen auf etwa 50 vernetzten PC für 2 Tage notwendig. Es gibt jedoch auch bereits spezielle Rechner-Hardware, die in einen Reisekoffer passt und in der gleichen Zeit den nötigen Schlüsselcode berechnen kann. Es ist also denkbar, dass z.B. **im Kino oder im Zug** jemand im Abstand von einigen Metern den Transponder des Fahrzeugschlüssels **unbemerkt ausliest**, um dann später aus den gewonnenen Signalen den Schlüsselcode auszurechnen. Danach ist es dem Angreifer möglich, das Fahrzeug zu öffnen und auch damit wegzufahren.

Außerdem gibt es **mit direktem Zugriff auf den Schlüssel** eine weitere Möglichkeit, über Messungen direkt an den im Schlüssel verwendeten Bauteilen den geheimen Code zu rekonstruieren. Bei dieser sog. Seitenkanalattacke kann der im Chip ausgeführte **Verschlüsselungscode** aus den Änderungen des Stromverbrauches gewonnen werden. Für die Durchführung dieser Messungen wird der **Original-Fahrzeugschlüssel nur für einige Minuten benötigt**. Mit der Schlüsselkopie lässt sich dann das Fahrzeug zwar öffnen, zum Deaktivieren der Wegfahrsperre sind dann aber evtl. noch weitere Maßnahmen notwendig.

3. Mechanisches Öffnen des Fahrzeugs und Anlernen eines neuen Schlüssels

Zusätzlich zu den hier vorgestellten elektronischen Manipulationen muss berücksichtigt werden, dass das mechanische Türschloss auch bei aktuellen Fahrzeugen **keine Hürde** für Profis wie z.B. **Schlüsseldienste oder Abschleppunternehmen darstellt**. Übliche Schlösser sind mit entsprechender Fachkenntnis und dem richtigen Werkzeug innerhalb von Minuten zerstörungsfrei zu öffnen. Mit einer Manipulation des Zündschlosses kann dann durch Einsatz entsprechender Software über die **OBD-Schnittstel-**

le (On Board Diagnosis) ein neuer Schlüssel angelernt werden, mit dem ein Diebstahl des Fahrzeuges möglich ist. In vielen Fällen ist hierzu ein besonderes **Herstellerpasswort** notwendig, welches nur ausgewählten Fachwerkstätten zur Verfügung steht. Es ist jedoch davon auszugehen, dass dieses den Fahrzeugdieben ebenfalls bekannt ist.

Falls das Fahrzeug nach dem Diebstahl wieder aufgefunden wird, kann durch **Analyse der elektronischen Steuergeräte** ggf. nachgewiesen werden, dass ein zusätzlicher Schlüssel angelernt worden ist. Oft sind bei einer Untersuchung des mechanischen Türschlosses mithilfe eines Mikroskops Spuren eines mechanischen Eingriffs nachzuweisen.

Bei einigen Fahrzeugherstellern wie bspw. Mercedes-Benz oder BMW ist man dazu übergegangen, dass kein Schlüssel angelernt werden kann, der nicht **vorher vom Hersteller speziell für das Fahrzeug codiert** worden ist. Die Schlüssel werden beim Hersteller auf Anfrage nach Einreichung von Fahrzeugschein und Kopie des Personalausweises angefertigt. Auf diese Weise wird wirksam verhindert, dass ein zusätzlicher Schlüssel ohne Registrierung beim Hersteller angelernt werden kann.

4. Ausblick – verschlüsselte Vernetzung der Steuergeräte im Fahrzeug

Heutige Fahrzeuge sind in zunehmendem Maße mit einer Vielzahl von Steuergeräten ausgestattet, deren Software einen immer wichtigeren Teil der Kostenbilanz eines Fahrzeugs einnimmt. Um Steuergeräte und insbesondere die darin gespeicherte Software vor Diebstahl und Manipulation zu schützen, werden an vielen Stellen bereits **kryptografische Verfahren** eingesetzt. Dabei sind primär folgende Punkte notwendig:

- **Datenschutz**: Gespeicherte und übertragene Daten sollen nur von oder mithilfe von authentifizierten Geräten erreichbar sein;
- **Datenintegrität**: Daten dürfen nur unter bestimmten Voraussetzungen von authentifizierter Stelle geändert werden, eine Änderung muss erkennbar sein;
- **Nachvollziehbarkeit der Quelle**: Der Ursprung von signierten Daten muss eindeutig feststellbar sein, um den Urheber einer Änderung nachvollziehen zu können.

Da die Kosten für die einzelnen Steuergeräte in Fahrzeugen sehr genau kalkuliert werden müssen, ergeben sich je nach Dateninhalt, Rechenleistung und Speichergröße **unterschiedliche Voraussetzungen** für die Umsetzung kryptografischer Verfahren. Für zentrale Einheiten wie z.B. das Motorsteuergerät ist bereits heute ein **Softwareupdate mit digitaler Signatur** notwendig, dessen Echtheit vom Steuergerät selbst vor dem Aktualisierungsvorgang überprüft wird. Auf diese Weise werden Manipulationen durch einfaches Austauschen der Steuergerätesoftware deutlich erschwert. Allerdings muss es auch möglich sein, für die Diagnose von Fehlern für die Werkstätten Möglichkeiten zu bieten, in diese Systeme eingreifen zu können.

Für **Multimedia- sowie Navigationsanwendungen** im Fahrzeug werden bereits heute leistungsfähige Verschlüsselungsalgorithmen eingesetzt, die die nachträgliche kostenpflichtige **Freischaltung zusätzlicher Funktionen** (bspw. TV-Tuner oder zusätzliches Kartenmaterial) ermöglichen, ohne eine einfache Manipulation durch Dritte zuzulassen.

In Zukunft sind für Fahrzeuge **vollständig verschlüsselte Bussysteme** und immer leistungsfähigere Verschlüsselungstechniken zu erwarten.

III. Zusammenfassung

Das Kopieren und Manipulieren von Fahrzeugschlüsseln und Wegfahrsperren ist ein Thema, das vielerorts diskutiert wird. Obwohl die Angaben **dubioser Firmen** im Internet, Schlüselkopien für jeden Fahrzeugtyp anfertigen zu können nicht überprüft werden können und in vielen Formen mit Halbwissen diskutiert wird, gibt es technische Möglichkeiten, entsprechende Möglichkeiten durchführen zu können. Für eine entsprechende Analyse ist es jedenfalls erforderlich, jedes **Fahrzeugmodell speziell** zu untersuchen. Falls das Fahrzeug nach der Entwendung nicht wieder aufgefunden wird, ist ein Nachweis eines Diebstahls durch technische Manipulation nur in wenigen Fällen möglich.

In vielen Fällen ist es einfacher, das Fahrzeug nicht wegzufahren, sondern das Fahrzeug direkt **auf einen Lkw oder Container zu verladen**, um es dann später so zu manipulieren, dass ein Weiterfahren möglich ist. Ein Container kann gleichzeitig die Diebstahlmeldung eines evtl. vorhandenen GPS-Ortungssystems unmöglich machen. Oft muss lediglich eine evtl. vorhandene **Alarmanlage** deaktiviert werden. Dies ist durch die unverschlüsselte Kommunikation auf den fahrzeuginternen Bussystemen jedoch kein großer Aufwand.

Die technische Manipulation des Fahrzeugs an den Steuergeräten oder durch zusätzlichen Einbau von Modulen macht es möglich, ein Fahrzeug im **Rahmen einer Probefahrt** so zu manipulieren, dass es zu einem späteren Zeitpunkt gestohlen werden kann.

Es ist zu erwarten, dass sich das **Wettrüsten** zwischen Fahrzeugherstellern und Fahrzeugdieben fortsetzt. Bereits jetzt ist erhebliches Know-how vonseiten der Fahrzeugdiebe notwendig, aktuelle Fahrzeuge manipulieren oder entwenden zu können. Erst **verschlüsselte Bussysteme** in den Fahrzeugen können die Hürden für die Fahrzeugdiebe so hoch legen, dass sich ein Diebstahl **ohne Zugriff auf den Schlüssel nicht mehr lohnt**.

Bereits jetzt ist der Trend festzustellen, dass nicht nur das Fahrzeug selbst, sondern durch einen **Wohnungseinbruch** oder einen **Überfall** die Schlüssel gleich mit gestohlen werden, sodass der gesamte technische Aufwand zur Überwindung der Fahrzeug-Sicherheitseinrichtungen entfällt.