Elektronische Fahrzeugschlüssel als Sicherheitsproblem?
Teil 1 – Grundlagen

*von Dr. Ingo Holtkötter, Münster**

Der Trend, Fahrzeuge mit elektronischem Schlüssel und Fernbedienung auszustatten, hat mittlerweile auch das günstigste Marktsegment erreicht. Speziell bei Fernbedienung und Wegfahrsperre ist die Sicherheit des Systems für den Anwender kaum noch zu beurteilen. Da die Kommunikation zwischen Schlüssel und Fahrzeug unsichtbar erfolgt und damit auch unbemerkt und ohne sichtbare Spuren zu hinterlassen durchgeführt werden kann, stellt sich nicht nur bei Fahrzeugdiebstählen die Frage, wie hoch die Sicherheit dieser Schließsysteme tatsächlich ist.

Im vorliegenden Artikel werden die Grundlagen und die Funktionsweisen zu verschiedenen Fernbedien- und Zugangssystemen beschrieben. Ein weiterer Artikel wird sich mit Sicherheit und Manipulationsmöglichkeiten dieser Systeme befassen.

I. Einleitung

1. Zugangsberechtigung, Fahrberechtigung

Die Aufgabe eines Zugangskontrollsystems, nur autorisierten Schlüsseln den Zugriff auf das Fahrzeug zu ermöglichen, lässt sich in zwei Bereiche gliedern. Zum einen sorgt der Schlüssel für eine **Zugangsberechtigung** mithilfe der Fernbedienung oder des Schlüsselbarts in Kombination mit dem Türschloss. Zum anderen bewirkt er in Verbindung mit Wegfahrsperre sowie Lenkrad- bzw. Zündschloss eine **Fahrberechtigung**.

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

Diese beiden Aufgaben sind meist von einander getrennt, da hier unterschiedliche Techniken verwendet werden. Einzig das moderne und meist aufpreispflichtige Keyless-Go®-Verfahren weist hier Besonderheiten auf, die später noch erläutert werden.

Die Kombination Schlüsselbart/Türschloss bildet den mechanischen Teil zur Erlangung der Zugangsberechtigung, welcher jedoch je nach eingesetztem Schlüsselbartprinzip für professionelle Schlüsseldienste **keine Hürde** darstellt. Mit leicht erhältlichen Teilesätzen zu den verschiedenen Schlüsselbartreihen sind auch aktuelle Fahrzeugtüren innerhalb weniger Minuten mechanisch ohne Zerstörung zu öffnen. Der elektronische Teil, die Fernbedienung im Schlüsselgehäuse, ist deutlich schwieriger zu beurteilen, da hierzu Messgeräte und spezielles Know-how nötig sind.

2. Schlüsselcode

Von der elektronischen Fernbedienung wird ein Code an das Fahrzeug übermittelt, der in der Bordelektronik mit dem hinterlegten Code verglichen wird und bei positivem Ergebnis die **Zentralverriegelung entriegelt**. Der elektronische Code übernimmt die Funktion des Schlüsselbarts beim mechanischen System: Er legt durch ein Muster fest, welcher Schlüssel (Code) passt und welcher nicht. Das Prinzip der Codeübermittlung vom Schlüssel zum Fahrzeug ist herstellerabhängig, es lässt sich jedoch in zwei Kategorien einteilen: Bei der Infrarot-Fernbedienung wird wie bei der TV-Fernbedienung ein gepulstes Lichtsignal, bei der Funk-Fernbedienung ein Funksignal zum Fahrzeug übermittelt.

II. Fahrzeugschlüssel mit Infrarot-Fernbedienung

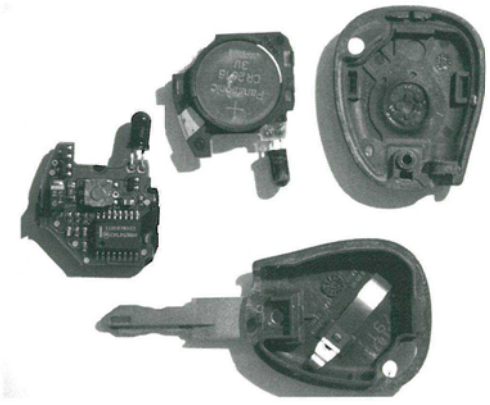

Abb. 1: Infrarot-Schlüssel eines Renault Scénic (Typ JA)

1. Infrarotsignal

Die Abb. 1 zeigt einen Schlüssel eines Renault Scénic Typ JA, der mit Infrarot-Technik ausgestattet ist. Neben der Batterie befindet sich im Schlüsselgehäuse noch eine Platine mit elektronischen Bauteilen, von denen das abstehende runde Bauteil die sog. Leuchtdiode ist, die genau wie eine **TV-Fernbedienung** die infraroten Lichtsignale zum Fahrzeug sendet. Mithilfe einer einfachen Handy- oder Pocketdigitalkamera kann man diese infraroten Lichtsignale sichtbar machen, da diese Kameras im Gegensatz zu hochwertigen und professionellen Kameras keinen Infrarotfilter besitzen. In Abb. 2 ist dies dargestellt: Das Infrarotsignal ist als heller Lichtfleck deutlich zu erkennen.

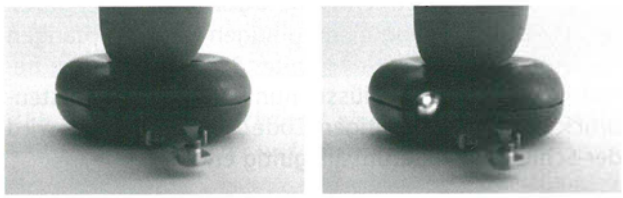

Abb. 2: Mit einer einfachen Digitalkamera sichtbar gemachtes Infrarot-Signal eines Schlüssels mit IR-Fernbedienung (Schlüssel eines Renault Scénic [Typ JA])

2. Festcode-Sender

Die erste Generation der Fahrzeugschlüssel mit Infrarot-Fernbedienung hat in den 1980er Jahren für einiges Aufsehen gesorgt: Mit Aufkommen der ersten lernfähigen und programmierbaren TV-Fernbedienungen ließ sich so mancher Fahrzeugschlüssel damit einlesen und fortan das Fahrzeug auch mit der TV-Fernbedienung öffnen. Die damals verwendeten sog. **Festcode-Sender** verwendeten zum Öffnen des Fahrzeugs immer denselben Code, sodass dieser Code nur einmalig aufgenommen werden musste, um jederzeit einen Zutritt in das Fahrzeug zu ermöglichen.

III. Wechselcodeverfahren

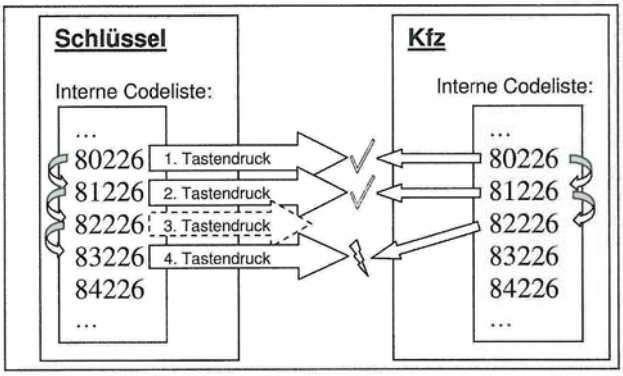

Abb. 3: Das Prinzip der Codeüberprüfung

Heutzutage werden aufwändigere Verfahren eingesetzt, die einfaches Kopieren der Schlüssel verhindern sollen. Hierzu wird beim **Wechselcodeverfahren** im Schlüssel bei jedem Tastendruck der zu sendende Code geändert, sodass sich der Code niemals oder sehr selten wiederholt. Aber woher weiß das Fahrzeug, welcher der nächste richtige Code sein wird? Das Prinzip der Codeüberprüfung ist in Abb. 3 erläutert. Der Schlüssel berechnet bei jedem Tastendruck mithilfe eines **geheimen Algorithmus** einen neuen Code. Dies ist hier durch eine Codeliste dargestellt, bei der sich die aufeinanderfolgenden Codes nur durch eine inkrementierte Ziffer unterscheiden. Der aktuelle Code sei „80226", beim nächsten Tastendruck wird der Code „81226" berechnet usw. Die Bordelektronik im Fahrzeug kennt den geheimen Algorithmus und kann sich

demzufolge die Reihe der Codes selbst berechnen. Beim ersten Tastendruck sendet der Schlüssel demzufolge den Code „80226", dieser stimmt mit dem im Fahrzeug berechneten Code „80226" überein und wird als gültig an die **Zentralverriegelung weitergeleitet**. Da das Fahrzeug einen gültigen Code empfangen hat, wird als nächstes der Code „81226" als gültig berechnet. Wenn der Schlüssel nun beim zweiten Tastendruck den neuen, richtigen Code „81226" sendet, wird der Schlüssel wiederum als gültig erkannt.

1. Codeverifikation

Wenn aber jemand z.B. in einem Gebäude außerhalb der Reichweite des Schlüssels versehentlich auf den Knopf drückt, berechnet der Schlüssel den nächsten Code, „82226", und sendet diesen aus. Da aber dieses Signal das Fahrzeug nicht erreicht, bleibt „82226" für das Fahrzeug weiterhin der gültige (und bisher ungenutzte) Code. Ein späterer vierter Tastendruck mit dem Schlüssel in der Nähe des Fahrzeugs könnte dann die Zentralverriegelung nicht mehr öffnen, da der Schlüssel dann „83226" sendet und die Bordelektronik immer noch „82226" erwartet. Um dieses Problem zu umgehen, ist die Bordelektronik des Fahrzeugs so programmiert, dass sie nicht nur den aktuellen Code, sondern auch bspw. die **255 nachfolgenden Codes akzeptiert**. Wichtig ist hierbei, dass ein neuerer Code die bisherigen Codes ablöst, d.h. dass ein wiederholtes Aussenden eines alten Codes nicht zum Erfolg führen kann. Andererseits kann es trotzdem passieren, den Schlüssel ungültig zu machen, wenn man versehentlich mehr als 255-mal den Knopf drückt, ohne dabei das Fahrzeug in Reichweite stehen zu haben. In so einem Fall ist der Schlüssel dann nicht mehr mit dem Fahrzeug synchronisiert und muss in der Werkstatt neu angelernt werden. Denken Sie also daran, wenn Sie den Schlüssel das nächste Mal Ihren (Klein-)Kindern zum Spielen in die Hand geben!

IV. Funktechnik für Fernbedienung und Wegfahrsperre

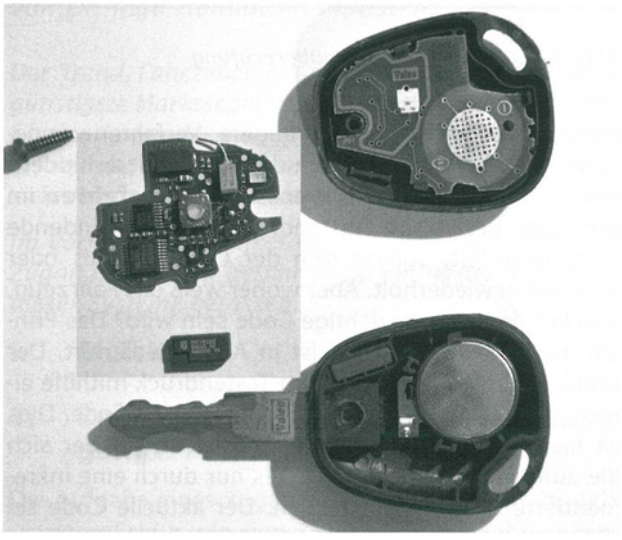

Abb. 4: Funkschlüssel eines Renault Laguna (Typ I) mit Transponderchip

Fahrzeugschlüssel mit Funktechnik, wie in Abb. 4 zu sehen, bieten für den Anwender einen erheblich höheren Komfort, weil die Codeübertragung und damit die Benutzung **erheblich weniger störanfällig** ist und der Schlüssel nicht mehr zum Fahrzeug gerichtet werden muss. Das Innere eines Funkschlüssels zeigt wieder eine große Batterie und eine Elektronikplatine, wobei die auffällige Infrarot-Leuchtdiode fehlt. Stattdessen wird das Funksignal über eine kleine Antenne abgestrahlt, die allerdings so kurz ist, dass sie auf die Platine passt. Bei den Funkschlüsseln werden ebenfalls Wechselcodesender verwendet, die wie oben beschrieben arbeiten.

Abb. 5: Funkschlüssel eines BMW E46 mit Transponderspule aus der Zündschlossbaugruppe

1. RFID-Transponder

Bei dem geöffneten Renault-Laguna-Schlüssel in Abb. 4 fällt noch ein zusätzliches Bauteil auf, welches nicht der Prüfung der Zugangsberechtigung, sondern im Zusammenhang mit der Wegfahrsperre der Prüfung der Fahrberechtigung dient. Der kleine schwarze Chip ohne elektrische Kontakte ist ein **RFID-Transponder**, der per Funksignal beschrieben und ausgelesen werden kann. Die RFID-Technik wird heutzutage in vielen Bereichen eingesetzt, z.B. als elektronischer Schlüssel bei großen Schließanlagen oder in Form von elektronischen Skipässen, die berührungslos die Abrechnung für den Ski-Lift ermöglichen. Diese Transponder sind so preiswert, dass sie sich auch im Einzelhandel als **Diebstahlschutz für günstige Produkte** bewähren.

2. Wegfahrsperre

Um die Kommunikation zwischen Fahrzeug und Transponder herzustellen, ist am Zündschloss eine **Sende-/Empfangsspule** angebracht. Abb. 5 zeigt die Transponderspule zusammen mit dem passenden Schlüssel eines BMW E46. Beim Starten des Motors wird über die Transponderspule ein Abfragesignal an den im Schlüssel befindlichen Transponder gesendet, dessen Antwort dann ggf. die Wegfahrsperre deaktiviert. Im Gegensatz zu den ersten Transpondergenerationen sind die in aktuellen Fahrzeugen verwendeten Transponder ausreichend intelligent und stromsparend, um auch **verschlüsselte Übertragungen** zuzulassen.

Abb. 6: Funkschlüssel eines Mercedes-Benz W202 mit bidirektionaler Schnittstelle zum Zündschloss statt Schlüsselbart und Transponder

3. Alternative zum Transponder

Abweichend vom Transponderverfahren hat der Fahrzeughersteller Mercedes-Benz bei einigen Modellreihen bis heute ein anderes Übermittlungsverfahren vom Schlüssel zur Wegfahrsperre bzw. zur Erlangung der Fahrberechtigung eingesetzt. In Abb. 6 ist ein Fahrzeugschlüssel der Baureihe W202 zu sehen, der zwar auch noch über einen herausschiebbaren mechanischen Schlüsselbart verfügt, der aber ausschließlich dazu dient, bei entladener Schlüsselbatterie das Fahrzeug mechanisch öffnen zu können. Dieser Schlüssel baut beim Einstecken in das vollelektronische Zündschloss eine **bidirektionale Infrarotverbindung** zur Fahrzeugelektronik auf. Um die Funktion des Schlüssels im Zündschloss unabhängig von der Schlüsselbatterie zu ermöglichen, wird über ein Magnetfeld eine Spannung in der Schlüsselelektronik induziert, um diese während der Benutzung mit Energie zu versorgen.

4. Komfortschließung

Die Infrarotsendedioden des Schlüssels werden auch zum Zweck der Fernbedienung verwendet: die Komfortschließung ermöglicht bei vielen Mercedes-Fahrzeugen, die Fenster und das Schiebedach zu bedienen, wenn der Schlüssel bei Tastendruck auf den Türgriff gerichtet wird. Hierzu befindet sich im Türgriff ein kleiner Infrarotempfänger, der die unmittelbare Nähe des Schlüssels detektieren kann.

V. Keyless-Go®-Verfahren

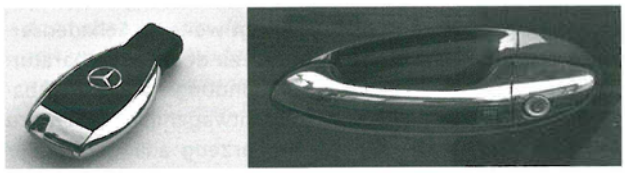

Abb. 7: Keyless-Go®-Schlüssel eines Mercedes-Benz W164 und Türgriff mit Taster und Infrarotempfänger

Nach einem völlig anderen Konzept funktioniert das Keyless-Go®-Verfahren, bei dem der Schlüssel nicht mehr in die Hand genommen werden muss, um ein Fahrzeug zu öffnen oder zu starten. Sobald sich eine Hand einem Türgriff eines entsprechenden Fahrzeugs nähert oder ggf. einen Taster am Türgriff betätigt, wird über ein Funksignal vom Fahrzeug der in der Nähe befindliche Schlüssel detektiert und abgefragt. Wenn dieser den richtigen Code zurücksendet, kann die Fahrzeugtür geöffnet werden. Das Anlassen des Motors geschieht dann auf ähnliche Weise: beim Drücken des Startknopfes wird wiederum der im Fahrzeuginnenraum befindliche Schlüssel abgefragt und bei positivem Ergebnis der Motor gestartet. Für dieses Verfahren muss das Fahrzeug mit mehreren Antennen ausgerüstet sein, um sehr genau erkennen zu können, ob sich der Schlüssel innerhalb oder außerhalb des Fahrzeugs befindet. Ansonsten könnte jemand an der Tankstelle den Motor starten und wegfahren, wenn der Besitzer des Schlüssels daneben steht und das Fahrzeug betankt.

VI. Sicherheit und Ausblick

Da bei diesem Verfahren die Kommunikation zwischen Schlüssel und Fahrzeug immer **bidirektional** ist, ist es als sehr robust und sicher einzustufen. Die anderen älteren Verfahren sind z.T. fehleranfällig, sodass Manipulationen denkbar sind. Die Fortsetzung dieses Artikels wird sich mit der Sicherheit der Systeme selbst und Manipulationsmöglichkeiten befassen.

(Beitrag wird fortgesetzt)

* VRR Entscheidungsservice: Die Volltexte der in dieser Ausgabe besprochenen Entscheidungen können kostenlos abgerufen werden unter: *www.burhoff.de* – Kennwort: Unfallschaden