Kai Rüsberg

Keyless gone

Autodiebe tricksen kontaktlose Schließsysteme aus

Technik soll Autos sicher und bequem machen, schon beim Einsteigen: Der Komfortschlüssel bleibt zum Öffnen der Tür und Starten des Motors in der Tasche. Doch leider ermöglichen diese Schließsysteme auch das komfortable Stehlen der Fahrzeuge.

Die beiden Nachbarn, die in Wöllstein in Rheinhessen leben, staunten nicht schlecht, als sie Ende August morgens mit ihren 5er BMWs losfahren wollten: Beide Fahrzeuge waren über Nacht verschwunden. Dabei waren keinerlei Spuren wie zersplittertes Fensterglas zurückgeblieben.

Die Bestohlenen hatten beim Kauf des Autos dieselbe Sonderausstattung bestellt: den Komfortzugang, die BMW-Variante des schlüssellosen Schließsystems. Die Polizei geht davon aus, dass die Täter dieses System überlistet haben und so die Fahrzeuge entwenden konnten, ohne Spuren zu hinterlassen.

Schlüsselloser Komfort

Die ersten Tür- und Zündschlösser, die auf das Einstecken eines Schlüssels verzichteten, hat Daimler 1999 in der S-Klasse angeboten. Heute haben alle Hersteller solche Systeme im Programm: Nicht nur in der Oberklasse, sondern bis hinunter zu den Kleinwagen sind die schlüssellosen Startsysteme gegen Aufpreis bestellbar.

Daimler hatte sich die Bezeichnung Keyless Go bereits 1998 als Wortmarke eintragen lassen. Inzwischen haben sich die Hersteller gut zwei Dutzend Bezeichnungen einfallen lassen: von Wortkreationen mit „Keyless“ (Hersteller wie VW, PSA, Suzuki) und „Komfort“ im Namen (BMW, Audi), über „Passive Entry“ (VDO, Hella, Bosch) bis zu Varianten von „Smart“ und „Intelligent Key“ (japanische und koreanische Hersteller).

Meist sehen die Keyless-Module wie ein herkömmlicher Autoschlüssel aus, nur fehlt der Metallbart. Bei einigen Fabrikaten sind aber auch Bauformen üblich, die einer zu dicken Scheckkarte oder einer dünnen Folienfernbedienung ähneln.

Die Systeme funktionieren über eine Funkverbindung im Nahfeld. Um das Auto zu öffnen oder zu schließen, muss man meist am Türgriff ein Sensorfeld berühren oder einen Taster drücken. Das Fahrzeug sendet dann ein schwaches Signal mit einer Reichweite von etwa einem Meter um die in Türnähe verbauten Niederfrequenz-Antennen. Der Schlüssel empfängt das Signal und prüft, ob es vom richtigen Fahrzeug stammt. Falls ja, sendet er wie ein gewöhnlicher Funkschlüssel ein hochfrequentes, verschlüsseltes Kommando, das die Türen entriegelt.

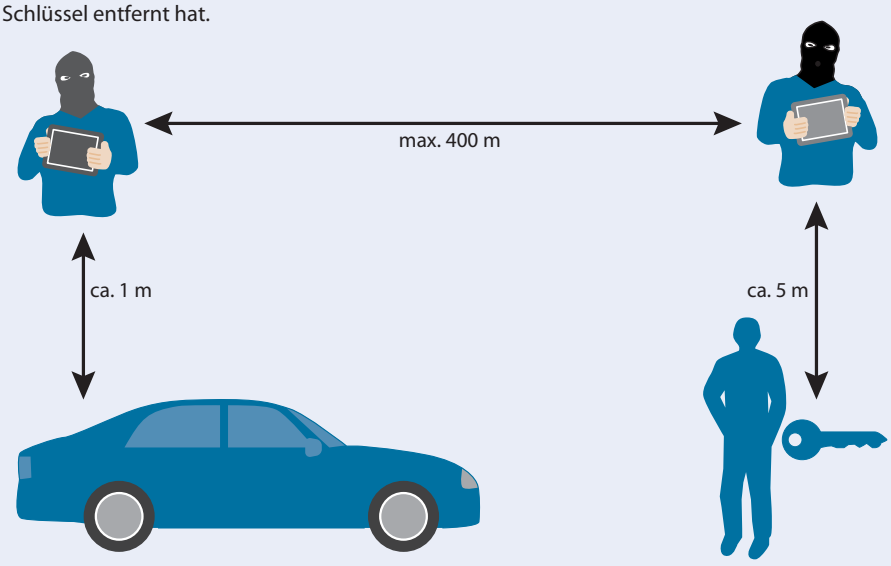
Im Inneren des Autos sind weitere Antennen verbaut. Erkennen sie, dass sich der Schlüssel im Wageninnern befindet, wird die Wegfahrsperre ausgeschaltet und der Startknopf für die Zündung freigegeben. Diese Kommunikation geschieht in Bruchteilen einer Sekunde und für den Autofahrer unmerklich.

Komfort für Diebe

Ebenso unmerklich können aber auch Diebe diese Kommunikation nutzen. Beim sogenannten Relais-Angriff (Relay Station Attack

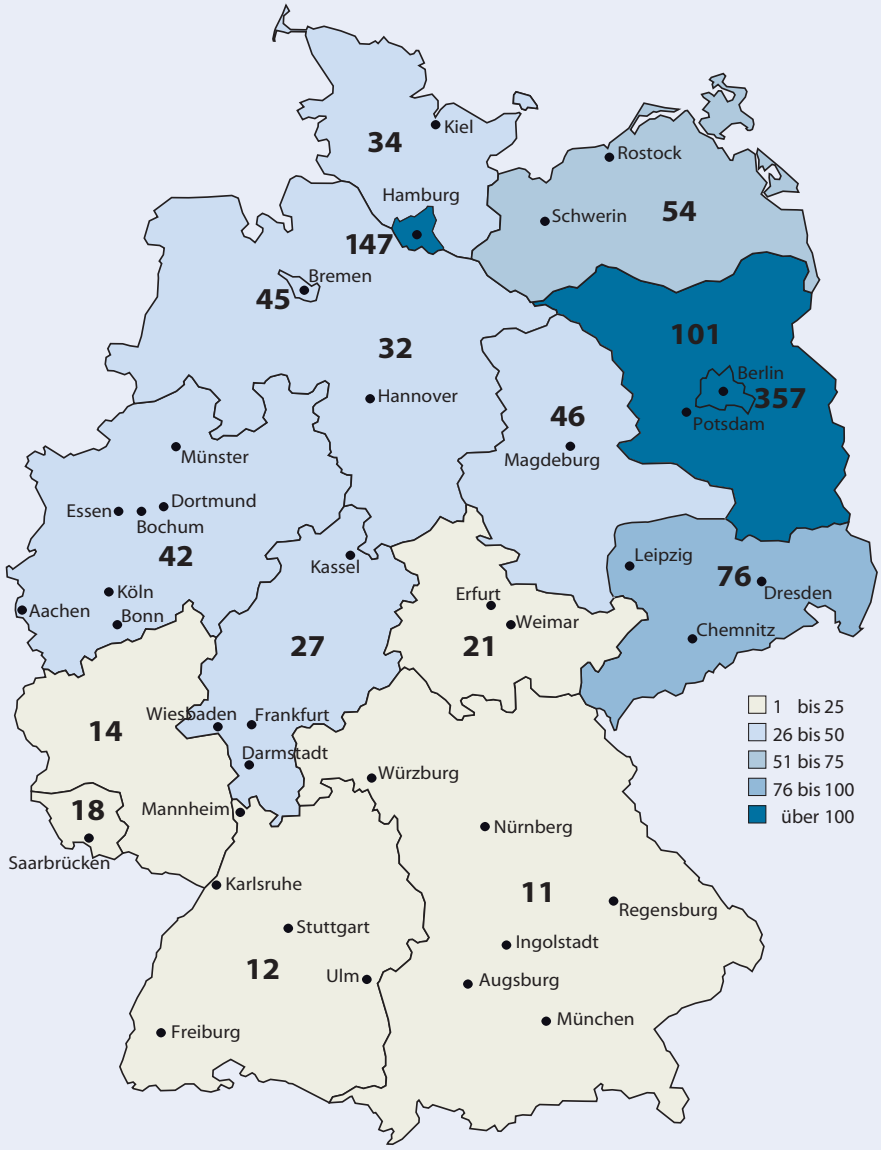
So nutzen Autodiebe schlüssellose Systeme

Der Autodieb und sein Komplize haben Funk-Relais dabei, die sich die Signale von Auto und Schlüssel gegenseitig weiterleiten. So kann der Dieb das Auto öffnen und starten, nachdem sich der Besitzer mit dem Schlüssel entfernt hat.



Dauerhaft entwendete Pkw

Nach Zahlen des Informationssystems der Polizei (INPOL) werden in den östlichen Bundesländern am meisten Fahrzeuge entwendet, während in der Heimat von Audi, BMW, Mercedes und Porsche das Blech sicherer ist. Die Zahlen zeigen die dauerhaft entwendeten Pkw je 100 000 zugelassener Fahrzeuge.



Quelle: BKA

oder RSA-Hack) reicht ein einfacher, aber wirkungsvoller Trick, um das Sicherheitssystem der Fahrzeuge auszutricksen. Anders als die Abkürzung RSA vermuten lässt, werden dabei die verschlüsselt übertragenen Daten nicht geknackt.

Vielmehr genügt es, die Reichweiten der Funksignale zu verlängern. Die sonst nur im Nahfeldfunk ausgetauschten Daten können so über viele Meter übertragen werden. Dabei kommt den Dieben zugute, dass die Hersteller der Funksysteme darauf verzichten, etwa anhand der Signallaufzeit die Entfernung zwischen Schlüssel und Auto zu überprüfen.

Diebe arbeiten derzeit mit zwei Varianten des RSA-Hacks. Bei der einfachen überträgt ein Relais-Funkgerät das niederfrequente 125-kHz-Signal von den Antennen des Autos an ein zweites Relais, das es unverändert abstrahlt. Das aktiviert den Schlüssel, der das Freigabesignal zum Entriegeln sendet. Diese Signale im 433-MHz-Band reichen einige Dutzend Meter weit – abhängig von Hindernissen zwischen Sender und Empfänger und je nach Ladezustand der Batterie.

Dieser Hack funktioniert also nur, solange sich der Fahrer mit dem Schlüssel noch in der Nähe des Autos aufhält. Starten lässt sich der Wagen aber nicht, da die Antennen im Wageninnern den Schlüssel nicht erkennen.

Dafür und für eine größere Reichweite muss das Relais-Funkgerät auch den Rückkanal mit einer zweiten Trägerfrequenz übermitteln. Der in Deutschland ansässige Hersteller eines solchen Systems namens „Q-Key2“ sagt, dass es Entfernungen bis zu 400 Metern überbrücken könne. Er verleiht die Systeme nach eigener Aussage allerdings nur an Bundes- oder europäische Ermittlungsbehörden für hoheitliche oder polizeiliche Zwecke.

Diebstahl in Sekunden

Der Angriff auf das Auto dauert nur wenige Sekunden. Außenstehende erkennen dabei nicht, ob der Dieb den Schlüssel oder einen anderen Funksender bei sich trägt. Es gibt kein Gefummel und keine Geräusche. Weil das Auto meint, der Originalschlüssel sei an Bord, kann der Dieb den Motor per Knopfdruck starten und mit dem Auto das Weite zu suchen.

Solange der Dieb den Motor nicht selbst ausstellt, kann er mit dem gestohlenen Auto auch weiterfahren, nachdem die Verbindung zum Schlüssel abgerissen ist. Die Keyless-Systeme schalten den Motor dann nicht ab. Das könnte während der Fahrt zu einem Unfall führen, etwa wenn die Verbindung zum Schlüssel im Auto durch einen technischen Defekt verloren geht. Ist das gestohlene Fahrzeug beiseite geschafft, können die Diebe mit speziellen Tools in Ruhe einen Nachschlüssel programmieren.

Die beiden Relais-Funkgeräte sind mit Antennen und Zubehör so klein, dass man sie unauffällig zum Beispiel in einer Laptop-Tasche verstecken kann. Das Relais auf Schlüsselseite kann das 433 MHz-Signal verstärken, um damit einige Meter zu überbrücken. Dann reicht es, wenn der Komplize des Diebs zum Beispiel an der Haustür steht, um den am Haken aufgehängten Schlüssel anzufunken.

Gelegenheiten gibt es für die Autodiebe viele: auf jedem Parkplatz, an Hotelrezeptionen oder Tankstellenkassen. Selbst wenn der Bestohlene sein Auto wegfahren sieht, dürfte ihm der Komplize in der Nähe, der die Schlüsseldaten abgegriffen hat, kaum auffallen.

Keine Reaktion

Bislang haben die Autohersteller auf dieses Angriffsszenario nicht reagiert. Dabei ist es bereits seit fünf Jahren bekannt. Drei Forscher der ETH Zürich schafften es 2010, mit einem Antennenpaar das Signal des Autos zum Schlüssel weiterzuleiten. Damit gelang ihnen das Fernöffnen auf eine Distanz von rund 100 Metern – so weit reichte das Signal des Schlüsselanhängers zum Fahrzeug zurück. Eine Antenne musste dabei sehr nah am Fahrzeug angebracht sein, die zweite befand sich maximal acht Meter vom Schlüsselanhänger entfernt. Zunächst testeten sie die Übertragung mit einer Kabelverbindung. Anschließend hatten sie auch mit einer Funkverbindung Erfolg. Die Studie wurde im Februar 2011 veröffentlicht.

Mittlerweile nutzen auch Diebe diese Technik offenbar zunehmend, um vornehmlich Autos der gehobenen Preisklassen zu

stehlen. Es gibt jedenfalls Polizeidienststellen, die eigenständig Verdachtsfällen nachgehen, in denen Keyless-Systeme überlistet wurden.

Die Polizei Südosthessen in Offenbach spricht von „konkreten Hinweisen“ auf solche Diebstähle. Im ersten Halbjahr 2015 ordnet sie 40 Diebstähle der Methode zu. Darunter waren mehrere BMW–Modelle der 5er-Reihe sowie Premiummodelle von Audi und Range-Rover. Mehrfach wurden gleich zwei Autos in unmittelbarer Nähe gestohlen, die Taten geschahen zwischen 0 und 4 Uhr nachts und alle Tatorte lagen in der Nähe von Autobahnanschlüssen. In dieses Muster passen auch die sechs Fälle Ende August in Rheinhessen, zu denen auch die beiden in Wöllstein gehören.

Autoschlüssel wie dieser des Renault Kadjar sehen eher aus wie Fernbedienungen. Den Schlüsselbart sucht man vergebens, ebenso wie das Schlüsselloch am Auto.

Nach dem Lagebild des Bundeskriminalamts zur Kfz-Kriminalität vom August 2015 gehören Berlin, Brandenburg, Sachsen und Hamburg prozentual zu den am stärksten von Pkw-Diebstählen betroffenen Ländern. Eine Anfrage bei den jeweils zuständigen Landeskriminalämtern ergab jedoch gleichlautend: Zu Diebstählen per RSA-Hack liegen keine Daten vor. Denn dieses Merkmal wird bei der Erstellung der amtlichen Statistik nicht abgefragt. Zudem hat die Polizei das Problem, dass üblicherweise keinerlei Beweise auf die Tatausübung zurückbleiben. Eine mögliche Ausnahme sind Videos von Überwachungskameras, die den Diebstahl filmten. Solche Aufnahmen gab es nach Recherchen von c’t in Hessen.

Wenig Klarheit

Außer den bestohlenen Eigentümern sind auch die Versicherungen betroffen. Eine Anfrage beim Gesamtverband der Deutschen Versicherungswirtschaft führt jedoch nicht weiter: „Statistiken zur Diebstahlhäufigkeit von Autos mit Keyless-System erhebt der Verband nicht“, so der GDV. Ähnlich verlaufen auch Anfragen an die HUK Coburg: „Derzeit kein Thema“ und bei der Allianz: „Wir beobachten das, können aber keine Aussage machen.“

Währenddessen entwickelt sich der Markt für Relais-Funkgeräte. Vor zwei Jahren wurden sie erstmals angeboten. Glaubt man Insidern kosteten sie noch im letzten Jahr mehrere 10 000 Euro. Nun gebe es Händler, die sie für etwa 1000 Euro verkaufen. Laut Boris Danev, einem der Mitarbeiter an der ETH Zürich, die 2010 das Sicherheitsproblem aufdeckten, könnten die Geräte noch billiger werden. Er forscht zurzeit an einer Version, deren Bauteile weniger als 100 Euro kosten sollen.

Die Funkgeräte müssen technisch in der Lage sein, die Daten ohne große Zeitverzögerung zu übermitteln. Eine genaue Prüfung, ob sich der Schlüssel in der Nähe des Autos befindet, lässt sich bei den seit Jahren unverändert verbauten Türschließsystemen nicht nachrüsten.

Selbstschutz

Der einfachste Weg, die Diebe mit dem RSA-Hack ins Leere laufen zu lassen, ist laut dem

Bochumer Sicherheitsforscher Timo Kasper, die Batterie aus dem Schlüssel zu nehmen. Damit sperrt man sich bei Systemen ohne Bart und Schloss aber selbst aus. Und für ständiges Ein- und Ausbauen der Batterie eignen sich die fummeligen Schlüsselgehäuse nicht.

Das LKA Rheinland-Pfalz rät dazu, den Schlüssel in Alufolie einzuwickeln. Das hilft nach unseren Versuchen tatsächlich; das ständige Ein- und Auspacken ist aber kaum praktikabel. Alternativ empfiehlt das LKA, den Schlüssel in einem Metallkasten aufzubewahren.

Der Bochumer Versicherungsagent Detlef Schuhmann hat das ausprobiert. Dabei fiel ihm auf, dass längst nicht jede Metalldose die Funkwellen abschirmt. Eine bunte Bonbondose hatte keine abschirmende Wirkung, während eine kleine Pralinendose das gewünschte Ergebnis zeigte: Das Auto ließ sich nicht mehr öffnen. Doch so eine Bastellösung hat mit Komfort nichts mehr zu tun.

Kein Komfort: Um den Schlüssel abzuschirmen, kann man ihn in einer Blechdose transportieren. Dazu eignet sich jedoch längst nicht jede Dose, man muss probieren.

Der Relais-Hack ist für die Sicherheitsingenieure der Automobilindustrie ein Desaster. Da denken sie sich komplizierte kryptografische Verfahren aus, um die Signale fälschungssicher zu machen. Und dann kommen Forscher daher und umgehen das mit einem simplen Trick.

Skandal

Zum Skandal wird das Ganze aber erst dadurch, wie die Hersteller damit umgehen. Bereits Anfang 2011 haben die Forscher von der ETH ihre Ergebnisse veröffentlicht. Doch die ersteller verkaufen immer mehr von dieser unsicheren Technik. Für ein paar hundert Euro können Kriminelle einfach zu bedienende Geräte kaufen und damit eine beachtliche Gewinnspanne erzielen.

Den Schaden haben nicht die Autohersteller, die für jeden gestohlenen Wagen möglicherweise sogar einen neuen verkaufen. Die Versicherer legen die Kosten per Typenklasseneinstufung ebenfalls auf die Kunden um. Und bei der Polizei ignoriert man das Treiben dieser neuen Masche bislang fast flächendeckend. Lediglich in Südost- und in Rheinhessen haben einige Beamte aus eigenen Stücken angefangen, die dreiste Diebesmasche zu ermitteln und in Strafanzeigen aktenkundig zu machen. (ad@ct.de) c't