Experten warnen: Digitale Autoschlüssel sind einfach zu knacken

Autodiebstahl: gehackt statt aufgebrochen

München, 27. November 2012 Autoschlüssel mit integriertem Sender müssen sicher und abgeschirmt verwahrt werden. Darauf haben Experten in einer Fernsehsendung auf Sat 1 hingewiesen. Dort wurde gezeigt, wie einfach die elektronische Diebstahlsicherung auszuhebeln ist.

Viele Autos sind heute mit einer schlüssellosen Zugangskontrolle (zum Beispiel „Keyless go“ oder „Komfortzugang“) ausgerüstet. Statt einem mechanischen Tür- und Zündschloss kommt dabei ein Funkchip zum Einsatz. Dieser baut zur Authentisierung eine Kommunikation mit dem Empfänger im Auto auf. Der Fahrer braucht nur noch einen Tür- oder Kofferraumgriff zu betätigen, dann wird die Verrieglung geöffnet, und das Fahrzeug kann mittels Startknopf angelassen werden. Es reicht, wenn sich der digitale Schlüssel in der Nähe des Fahrzeugs befindet.

Dass diese Methode keineswegs sicher vor Hackern ist, wurde von Spezialisten in der Sendung „Akte 20.12“ eindrucksvoll bewiesen. Es ist nämlich durchaus möglich, sich dem Autobesitzer, zum Beispiel in einem Restaurant, unbemerkt zu nähern und mit einem frei erhältlichen Lesegerät eine Funkkommunikation zum digitalen Autoschlüssel aufzubauen.

Die Kommunikationsdaten leitet der Hacker dann über eine Funkstrecke an seinen Komplizen weiter, der vor dem zu knackenden Auto steht. Dieser hat einen weiteren Sender und Empfänger dabei, der die Schlüsseldaten dann weitergibt. Im Test konnte der Hacker-Komplize einfach einsteigen und davonfahren.

„Diese Hacker-Strategie ist eigentlich nichts Neues“, weiß Stefan Horvath, Managing Director von Kryptronic. Sein Unternehmen befasst sich schon seit vielen Jahren mit der Abschirmung von Sicherungssystemen gegen nicht autorisiertes Auslesen. „Es handelt sich um einen so genannten Relais Station Attack (RSA)“, so Horvath weiter. „Dabei überbrückt ein Hacker einfach die Entfernung zwischen Fahrzeug und Schlüssel. Die Kommunikationsdaten werden unverändert weitergeleitet. Der Empfänger im Fahrzeug kann nicht unterscheiden, ob sich der digitale Schlüssel tatsächlich in der Nähe befindet, oder ob das Signal nur künstlich ‚verlängert‘ wurde.“

Das grundlegende Sicherheitsproblem sei dabei dasselbe wie auch bei Bank- oder Kreditkarten mit NFC-Chip. „Die Funkmodule können nicht erkennen, ob ein Sicherheitssystem oder ein Ganove die Kommunikation initiiert hat“, erklärt Stefan Horvath. „Der Chip antwortet grundsätzlich jedem, der digital anklopft.“

Dennoch zieht auch Horvath das System nicht generell in Zweifel. „Schlüssellose Zugänge sind praktisch und können mit geringem Aufwand gegen unberechtigte Kommunikation abgeschirmt werden – genauso wie NFC-Kredit- oder -Bankkarten.“

Für die Abschirmung wird nicht selten eine selbst gebastelte Hülle aus gewöhnlicher Aluminiumfolie empfohlen. Doch davon raten Sicherheitsexperten dringend ab. Der Schlüssel muss zum Aufsperren immer wieder umständlich ausgewickelt werden. Dabei reißt die Folie oft, und die Hülle wird unbrauchbar. Und selbst eine intakte Schicht aus normaler Haushaltsfolie kann das Abgreifen der sensiblen Daten oft nicht verhindern.

Wirklich sicher und praktikabel sind nur Abschirmungen aus einem Spezialmaterial. Eigens zu diesem Zweck wurde daher von Kryptronic die Metalllegierung Cryptalloy entwickelt. Sie wird zu einer nur 0,1 Millimeter dicken Folie verarbeitet, mit einem Schichtträger aus reißfestem PET-Kunststoff. Cryptalloy-Folie schützt vor jedem Leseversuch – auch dann, wenn sie das Objekt nicht umschließt. Es gibt sie bei Kryptronic für gewerbliche Kunden als Meterware. Fertige konfektionierte Hüllen für den Endverbraucher werden für wenige Euro in diversen Online-Shops angeboten. Dort gibt es auch mit Cryptalloy abgeschirmte Schlüsseletuis. Sie sind nur wenig teurer als gewöhnliche Modelle, können aber den digitalen Autodiebstahl zuverlässig verhindern.

Auch viele Geldbörsen, Kreditkarten-Fächer oder Ausweisetuis werden mittlerweile schon mit Cryptalloy-Abschirmtechnik geliefert. Jeder Hersteller kann seine Cryptalloy-Produkte bei Kryptronic laborphysikalisch testen und zertifizieren lassen.

Bildmaterial, Produktmuster und -präsentationen, persönliche Pressegespräche oder Fachartikel jederzeit auf Anfrage

Kryptronic
Kryptronic Technologies, hat sich seit der Gründung im Jahre 1995 als Ausrüster und Zulieferer von Präzisionsoptiken und NFC-Shielding-Technologie einen Namen gemacht. Das Unternehmen mit Firmensitz in München unterhält ein eigenes Entwicklungs- Mess- und Prüflabor, in dem Cryptalloy-Produkte individuell zertifiziert werden. Kryptronic Technologies liefert seine Produkte an mehr als 2000 Kunden in Medizin, Forschung und Industrie. www.kryptronic.de

Cryptalloy
Cryptalloy ist eine von Kryptronic speziell für die RFID und NFC-Abschirmung (NFC: Near Field Communication) entwickelte Aluminium-Legierung, die auf einem hochreißfesten Schichtträger aus PET aufgebracht ist. Cryptalloy kann wie eine normale Alu-Verbundfolie verarbeitet werden und verhindert zuverlässig das nicht autorisierte Auslesen von Informationen. Cryptalloy ist als unverarbeitete Folie erhältlich, aber auch in einer Vielzahl von Produkten, zum Beispiel Ausweistaschen, Werbeartikel, Geldbörsen, Schlüssel- oder Kreditkartenhüllen.
www.cryptalloy.de

Pressekontakt:

Siebler kreativ
Ralf Siebler
(089) 307 26-216
rs@siebler-kreativ.de
www.siebler-kreativ.de

Kontakt für Händleranfragen:
Cryptalloy Berlin

Dirk Stöppel
(030) 34 65 96 49
ds@cryptalloy.de