

Neue Software knackt Autos und Wegfahrsperrre!



Autoklau-Software

Knackt alle Autos!

Stellen Sie sich vor: Ihr Auto ist nicht mehr da, wo es sein sollte. Es wurde geklaut. Normalerweise gehen Sie zur Polizei und zeigen den Diebstahl an.

Relativ unglaublich ist der Autoklau für die Polizei, wenn Ihr Wagen eine verschlüsselte Funkübertragung nutzt. Etwa zum Öffnen der Wagentür mit dem Zündschlüssel. Denn nur wenn die Daten richtig verschlüsselt sind, öffnet das Auto die Tür. Aber damit nicht genug: Im Autoschlüssel ist oft ein Funkchip eingebaut, der weiterhin mit dem Auto „spricht“. So können Sie etwa den Wagen nur starten, wenn der Funkschlüssel die richtigen Daten an den Wagen „sendet“ (die sogenannte Wegfahrsperrre).

Wird so ein solches „absolut sichere“ Auto geklaut, vermutete die Polizei erst einmal Versicherungsbetrug. Denn eigentlich kann das Auto gar nicht gestohlen werden, da es nicht ohne den richtigen Schlüssel-Code fahren kann.

RUHR-UNIVERSITÄT BOCHUM

Funktüröffner für Autos und Gebäude geknackt
RUB-IT-Sicherheitsexperten decken massive Schwachstelle auf
Zugang ohne Spuren aus 100 Metern Entfernung

Wissenschaftler der Ruhr-Universität Bochum haben die auf der weit verbreiteten KeeLoq RFID-Technologie basierenden Funktüröffnersysteme geknackt. Die aufgedeckte Sicherheitslücke besteht bei allen Autoschlüsseln und Gebäudezugangskontrollsystemen, die auf KeeLoq

Bochum,
Nr. 87

■ Diese Pressemeldung der Ruhr-Universität ließ die Bombe platzen. Die angeblich absolut sicheren elektronischen Autoschlösser sind geknackt. Sogar die Garage, in der das Auto steht, kann mit einem passenden Schlüssel geknackt werden.



Verschlüsselung ist geknackt

Wissenschaftlern der Ruhr-Universität Bochum ist es nun gelungen, die bei der Verschlüsselung übertragenen Daten zu entschlüsseln. Sie mussten dazu einfach abwarten, bis jemand sich seinem Auto näherte. Dabei konnten die Wissenschaftler sich bis zu 100 Meter vom Auto entfernt befinden. Dann mussten Sie nur noch die Funkübertragung zwischen dem Zündschlüssel und dem Auto abfangen. Und zwar in dem Moment, indem der Autobesitzer am Schlüssel die

Taste zum Öffnen der Tür betätigt. Die geknackte Verschlüsselung nennt sich „Kee-Log“ und wird bei vielen Automarken wie etwa Toyota eingesetzt.



Generalschlüssel für alle Marken

Durch das Abfangen mehrerer Funkübertragungen zwischen Autos eines Herstellers ist es den Wissenschaftlern sogar gelungen, einen Generalschlüssel für eine Automarke herzustellen. Es ist sogar möglich, ein Auto so zu manipulieren, dass der Funkschlüssel geändert wird. Dann

können Sie Ihr Auto nicht mehr öffnen. Aber Hacker schon.



Auch Garagentore sind in Gefahr

Aber nicht nur Autos sind in Gefahr. Denn das „Kee-Log“-Verfahren wird auch bei elektronisch öffnen den Garagentoren verwendet. Und bei Sperrtoren zu Grundstücks-Einfahrten. Damit können sich Kriminelle sogar Zugang zu Ihrer Garage oder sogar ins Haus verschaffen. Und dann weisen Sie mal bei der Polizei einen Einbruch nach, wenn überhaupt keine Einbruchspuren zu finden sind.



Schweigen bei den Autoherstellern

„Computer – Das Magazin für die Praxis“ hat bei den führenden Herstellern nachgefragt. Wird es eine Rückrufaktion geben? Zu dieser Frage gab es keine eindeutigen Antworten. Die Hersteller werden wohl erst reagieren, wenn etwa immer mehr angeblich „absolut sichere“ Autos geklaut werden. ■