Deutschlandfunk
Forschung Aktuell

Abhörsicherer Türöffner

Asymmetrische Verschlüsselung soll funkende Autoschlüssel sicherer machen

Autor: Ralf Krauter
Redakteurin: Uli Blumenthal
Länge: 4’15’’
Sendedatum: 28. 7. 2010

Moderation

Ein Druck auf den Knopf am Schlüssel und schon sind die Autotüren offen - Zentralverriegelung per Funk ist eine praktische Sache, auf die heute kaum noch einer verzichten mag. Nur: Sonderlich sicher ist die Funkverbindung nicht. Experimente zeigten: Mit Know-How und krimineller Energie lassen sich die übertragenen Daten abhören und entschlüsseln. Das ermöglicht es Autodieben, per Computer einen Zweitschlüssel zu erstellen. Um ihnen das Leben schwerer zu machen, haben Forscher in Garching jetzt einen Funkschlüssel mit einem neuartigen Kryptographie-Chip entwickelt. Ralf Krauter.

Beitrag

Autor

In die Hosentasche würde er nicht passen, der Funkschlüssel, den Johann Heyszl entwickelt hat. Noch nicht. Schließlich sei das Ganze nur ein Prototyp, erklärt der Forscher vom Fraunhofer-Institut für sichere Informationssysteme in Garching, nachdem er das Kästchen vom Format einer Butterdose auf den Tisch gelegt hat. Sein Herzstück, ein programmierbarer Prozessor, verschlüsselt die per Funk übertragenen Daten deutlich besser als heute üblich.

Zuspiel 1: O-Ton Heyszl, 01:05 – 01:20, 15s

Wenn man's wirklich produzieren würde, dann wäre diese Zusatzhardware, die jetzt etwas klobig wirkt hier, kleiner als ein Quadratmillimeter. Also das würde sich sehr sehr einfach integrieren lassen in einen bestehenden Schlüssel.

Autor

Um die Funktion der Fernbedienung zu demonstrieren, drückt Johann Heyszl abwechselnd auf einen ihrer beiden Knöpfe und zeigt auf den Monitor seines Laptops. Daran angeschlossen: Ein Empfängerchip, der später im Auto stecken würde.

Zuspiel 2: O-Ton Heyszl, 02:15 – 02:40, 20s

Der empfängt diese Nachricht von dem Prototypen-Funkschlüssel, entschlüsselt diese Nachricht, verifiziert die Daten. Und hier im Bildschirm sieht man dann: Das Auto, das hier dargestellt ist, das ist einmal gelockt und einmal open, je nachdem welchen Knopf man hier drückt an der Fernbedienung.

Autor

Heutige Funkschlüssel benutzen durchweg symmetrische Verschlüsselungsalgorithmen, um die Daten zu kodieren. Dabei wird der binäre Geheimcode zum Entschlüsseln der Übertragung stets an zwei Orten gespeichert: Im Schlüssel und im Auto. Das Problem dabei: Mancher Hersteller speichert in vielen Fahrzeugen denselben Geheimcode. Wurde dieser „Hauptschlüssel" erst einmal geknackt, haben Autodiebe bei einigen Fabrikaten leichtes Spiel.

Zuspiel 3: O-Ton Heyszl, 10:25 – 11:00, 25s

Wir gehen davon aus, nach unserem Wissensstand, dass es hier manufacturer keys gibt, die zum Beispiel für eine ganze Produktionslinie von Autos eingesetzt werden. Und da kann es dann passieren, dass wenn ein manufacturer key einmal geknackt wird, dass man dann eine ganze Reihe von Schließsystemen knacken kann aufgrund dessen.

Autor

Eine Art Domino-Effekt ist die Folge. Im Prinzip braucht ein Dieb nur auf einem Parkplatz zu warten, bis jemand ein baugleiches Auto per Funk verriegelt. Über eine Antenne kann er die Übertragung aus einigen Metern Entfernung belauschen und per Computer im Nu einen Nachschlüssel

machen. Forscher der Universität Bochum konnten zeigen, dass das mit etwas Know-How kein Problem ist.

Zuspiel 4: O-Ton Heyszl, 11:30 – 11:50, 15s

Denen ist es gelungen, dann auf Basis eines manufacturer keys, den sie knacken konnten, aufgrund nur weniger über Funk empfangener Nachrichten dann Schlüssel auch zu klonen.

Autor

Um Abhilfe zu schaffen, verwenden Hersteller heute Kryptographie-Algorithmen mit längeren binären Sicherheitsschlüssel, denn die sind schwerer zu knacken. Für die Experten in Garching ist das aber noch nicht die perfekte Lösung. Noch besser wäre es, glaubt Johann Heyszl, wenn das digitale Geheimnis nur noch im Schlüssel stecken würde und nicht mehr im Auto. Asymmetrische Kryptographie heißt das im Fachjargon.

Zuspiel 5: O-Ton Heyszl, 04:50 – 05:25, 30s

Asymmetrische Kryptographie bietet Vorteile im Management von diesem Schlüsselmaterial, weil also nicht mehr auf beiden Seiten Geheimnisse gespeichert werden müssen, sondern nur noch auf einer Seite – in dem Fall also wirklich bei dem Funkschlüssel. // Andererseits ist asymmetrische Kryptographie viel rechenaufwändiger. Uns ist es jetzt aber gelungen, den Rechenaufwand durch ein neues Protokoll soweit in Grenzen zu halten, dass es eigentlich gut möglich ist, das umzusetzen.

Autor

Das optimierte Rechenverfahren ist so stromsparend, dass die Batterie des asymmetrischen Funkschlüssels ähnlich lange durchhält, wie bei heutigen Autoschlüsseln. Etwas teuerer käme der Einsatz des neuartigen Krypto-Chips wohl, dafür wäre die Gefahr des Domino-Effektes gebannt. Selbst wenn es Autoknackern mit allerhand technischem Aufwand gelänge, einem der Funkschlüssel sein Geheimnis zu entreißen - sie könnten damit nur Nachschlüssel für ein einziges Auto herstellen. Da es keinen Hauptschlüssel mehr gibt, blieben ihnen alle anderen baugleichen Fahrzeuge verschlossen. Kein Wunder, dass sich Autobauer und Zulieferer interessiert zeigten, als Johann Heyszl den Prototypen seines asymmetrischen Funkschlüssels kürzlich auf einer Messe präsentierte.