



- » [Link zum Originalbild](#)
- » Copyright: News-Reporter.NET
- » Image-No.: 2010050024_0001

Verschlüsselt und doch nicht sicher. Asymmetrische Algorithmen sollen das Auto vor unliebsamen Zugriffen schützen. Foto: Fraunhofer Institut/auto-reporter.net

Trügerische Sicherheit – belauschte Funkfernbedienung

Funkfernbedienung für die Zentralverriegelung – Fluch und Segen zugleich, denn kaum ein Autofahrer möchte auf die Vorzüge einer solchen Fernbedienung für sein Fahrzeug verzichten, obwohl diese Technik in puncto Sicherheit Schwachstellen aufweist. Für Abhilfe soll nun ein asymmetrischer Algorithmus sorgen, wie er erstmals von Forschern am Fraunhofer-Institut programmiert und in einen Prototypen integriert wurde.

Bislang haben Autodiebe leichtes Spiel. Belauschen sie das Funksignal zwischen Fahrzeug und Fernbedienung über eine Antenne und erstellen aus den gewonnenen Daten per Computer einen Zweitschlüssel, stehen ihnen sozusagen die Türen vieler Autos offen.

Es gilt, Sicherheitslücken zu schließen, die sich durch zu schwache Algorithmen aufgetan haben. Deren Aufgabe ist es, vom Schlüssel zum Auto gesendete Informationen zu kodieren. Ihr Code ist bereits vor rund zwei Jahren geknackt worden. Neue Algorithmen kamen zum Einsatz. Aber auch sie haben Schwachstellen: Sie sind symmetrisch, sodass die „Geheimnisse“ sowohl im Schlüssel als auch im Auto hinterlegt sind. Und da ein und dasselbe Geheimnis in zahlreichen Fahrzeugen einer Produktionslinie gespeichert ist, lassen sich mit einem geknackten Schlüssel die Türen zahlreicher Autos öffnen.

Jetzt haben Forscher am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) in Garching einen asymmetrischen Algorithmus entwickelt, der die Verschlüsselung sicherer machen soll. „Bei dieser Art von Algorithmen befindet sich das Geheimnis nur im Autoschlüssel selbst, nicht jedoch im Auto“, sagt Johann Heyszl, Wissenschaftler am SIT. „In jedem Autoschlüssel steckt ein anderes Geheimnis, was diese Verschlüsselung sehr viel sicherer macht als die symmetrische.“

Die hohe Rechenintensität und der dadurch bedingte hohe Energieverbrauch sprachen bisher gegen den Einsatz solcher Algorithmen. Abhilfe schafft ein kleiner kryptographischer Chip, der besonders energiesparend ist, und ein neu entwickeltes effizientes Protokoll minimiert den Rechenaufwand und die zu übertragende Datenmenge. Mit dieser Lösung hält die Batterie im Schlüssel ähnlich lange wie bei der symmetrischen Verschlüsselung.

Auf die gleiche Art und Weise wie die Funkbedienung der Zentralverriegelung wird auch die elektronische Wegfahrsperrung verschlüsselt. Einen funktionsfähigen Prototypen haben die Forscher bereits entwickelt. Vom 2. bis 4. März stellen die Forscher das System auf der in Nürnberg stattfindenden Messe „embedded world“ vor (Halle 11, Stand 11-101). (auto-reporter.net/sr)