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

Presse-Info

Bochum, 31.03.2008
Nr. 87

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 basieren. „Die Schwachstelle ermöglicht es Unbefugten, sich aus 100 Metern Entfernung Zugang zu den ‚gesicherten' Fahrzeugen und Gebäuden zu verschaffen, ohne Spuren zu hinterlassen", erklärt *Prof. Dr.-Ing. Christof Paar*, an dessen Lehrstuhl für Kommunikationssicherheit (Fakultät für Elektro- und Informationstechnik) der Hack gelungen ist. Die Technik findet auch bei Garagentoröffnern und in der Ersatzteilsicherung Verwendung.

Zwei abgefangene Nachrichten genügen

Der Gruppe um Prof. Paar gelang es unter Einsatz modernster kryptanalytischer Verfahren, neue Angriffe zu entwickeln, die es z.B. erlauben, Autoschlüssel und Garagentoröffner auf eine Entfernung von bis zu 100 Metern zu klonen. „Das Abfangen von nur zwei Nachrichten erlaubt es Unbefugten, einen Schlüssel zu kopieren und sich Zugang zu Auto oder Haus zu verschaffen", sagt Prof. Paar. Mit einem anderen Angriff kann das Fahrzeug oder die Garage so manipuliert werden, dass die normalen Sender nicht mehr funktionieren und dem rechtmäßigen Besitzer der Zugang verwehrt wird.

Neuste kryptanalytische Methoden

Ein Funktüröffner besteht aus einem aktiven RFID-Sender, wie er typischerweise in Autoschlüssel eingebaut wird, und einem Empfänger, der sich in der Fahrzeugsteuerung befindet. Beide Seiten, Sender und Empfänger, verschlüsseln ihre Funk-Kommunikation mit der KeeLoq-Chiffre. Die Angriffe der Bochumer Gruppe ermöglichen die Rückgewinnung des geheimen Schlüssels sowohl auf der Sender- als auch auf der Empfängerseite, durch die Messung der elektrischen Energie, die die Geräte verbrauchen. Unter Anwendung der so genannten Seitenkanalanalyse konnten die Forscher den Herstellerschlüssel – eine Art Generalschlüssel für sämtliche Produkte einer Serie – aus dem gemessenen Stromverbrauch des Empfängers zurückgewinnen. Der Angriff, der Seitenkanalanalyse und spezielle Eigenschaften der KeeLoq-Chiffre kombiniert, kann auf alle bekannten Ausführungen der Chiffre, die in gängigen Systemen eingesetzt wird, angewandt werden. Die Verwundbarkeit wurde von der Bochumer Gruppe durch Angriffe auf kommerzielle Systeme überprüft.

KeeLoq: Weltweite Verbreitung seit Mitte der Neunziger

KeeLoq wird seit Mitte der neunziger Jahre standardmäßig in Zugangskontrollsystemen eingesetzt. Es ist eines der am weitesten verbreiteten Verfahren in Europa und den USA. Neben der häufigen Verwendung in Garagentoröffnern und Gebäudezugangskontrollsystemen wird KeeLoq auch von mehreren Automobilherstellern wie Toyota/Lexus als Diebstahlschutz eingesetzt.

IT-Sicherheitsforschung an der RUB

Die Gruppe um Prof. Paar ist Teil des Horst Görtz Instituts für IT-Sicherheit (HGI) an der RUB, eine der größten Forschungseinrichtungen für Kryptologie in Europa. Der Lehrstuhl von Prof. Paar ist eine der international führenden Gruppen im Bereich der Analyse und Sicherung von eingebetteten Systemen. Die Ruhr- Universität Bochum bietet das umfangreichste

Ruhr-Universität Bochum - Pressestelle - 44780 Bochum - Tel.: 0234/32-22830, -22930 - Fax: 0234/32-14136;
e-mail: josef.koenig@ruhr-uni-bochum.de - Internet: http://www.ruhr-uni-bochum.de/pressestelle/

BITTE, FOLGESEITE BEACHTEN

Ausbildungsprogramm für Sicherheit in der Informationstechnik (Bachelor, Master und Fernstudiengang) in Deutschland.

Prof. Dr.-Ing. Christof Paar, Lehrstuhl für Kommunikationssicherheit, Fakultät für Elektro- und Informationstechnik der Ruhr-Universität Bochum, 44780 Bochum, Tel. 0234/32-22994, E-Mail: keeloq@crypto.rub.de,
Mehr Informationen zum KeeLoq-Angriff: http://www.crypto.rub.de/keeloq
Lehrstuhl für Kommunikationssicherheit: http://www.crypto.rub.de
Horst Görtz Institut für IT-Sicherheit: http://www.hgi.rub.de

Weitere Informationen