

# Unsere Erfahrung ist Ihr Vorteil – die Division Automotive

Durch zahlreiche Projekte haben unsere Experten wertvolle Erfahrungen im Bereich Automotive Security gesammelt. Die Division Automotive der secunet deckt daher ein breites Spektrum an Themen ab.

## In-Vehicle-Security



- ▶ Komponentenschutz
- ▶ Wegfahrsperrren-Systeme
- ▶ Sicheres Flashen & Codieren
- ▶ Sichere Onboard-Kommunikation

## Secure Vehicle Communication

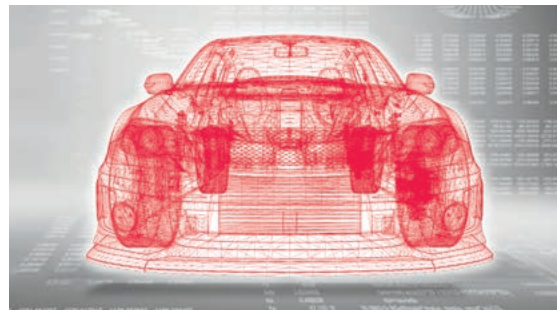


- ▶ Vehicle-to-Grid
- ▶ Car-to-Car Kommunikation
- ▶ Vehicle-to-Infrastructure

## Secure Remote Service Integration

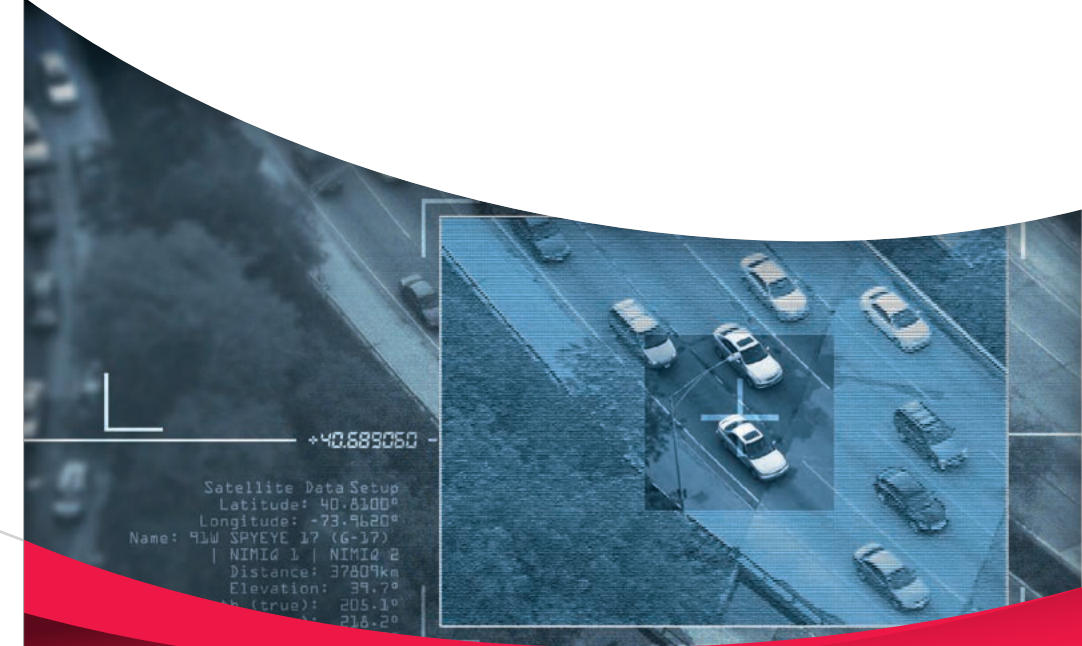


- ▶ Mobility Services / CarSharing
- ▶ Remote Access & Unlock
- ▶ Remote Update Service
- ▶ Online Services & Automotive  
Cloud Integration



# Penetrationstests Automotive

Professionelle Sicherheitsanalysen



## secunet

secunet Security Networks AG  
Kurfürstenstraße 58  
45138 Essen

[www.secunet.com](http://www.secunet.com)

Dr. Henning Daum  
Leiter Bereich Embedded Security  
Tel.: +49-201-5454-2115  
E-Mail: [henning.daum@secunet.com](mailto:henning.daum@secunet.com)  
Konrad-Zuse-Platz 2, 81829 München

## secunet

## Penetrationstests zur Aufdeckung von Schwachstellen im Fahrzeug

Durch die Digitalisierung und Vernetzung moderner Fahrzeuge sind Fahrer und Fahrzeug zunehmend Bedrohungen durch Cyber-Attacken ausgesetzt. Die gleichzeitig stetig steigende Bordnetz-Komplexität erhöht das Risiko erfolgreicher Angriffe und erschwert die Identifikation möglicher Schwachstellen und Fehlerursachen.

Ein erprobtes Verfahren zur Analyse der eingesetzten Sicherheitsmechanismen sind Penetrationstests. Hierbei wird nicht funktional getestet, sondern über systematische Untersuchungsschritte nach Angriffsflächen in Steuergeräten und Fahrzeugbordnetzen gesucht. Gefundene Schwachstellen werden anschließend hinsichtlich ihrer Ausnutzbarkeit und möglicher Auswirkungen bewertet und Gegenmaßnahmen aufgezeigt.

Mit einem hochwertig ausgestatteten Labor und eigener Untersuchungshalle für Fahrzeuge bietet secunet hierfür ein herstellerunabhängiges Testspektrum zur Analyse der Sicherheit von vernetzten Fahrzeugsystemen an, vom einzelnen Steuergerät bis hin zum Fahrzeug-Gesamtsystem.

## Unser Leistungsspektrum

- ▶ Untersuchungen der Robustheit von Protokollimplementierungen, Fuzzings
- ▶ Logische Angriffe, White-Hat-Hackings
- ▶ Reverse Engineerings
- ▶ Source Code-Analysen
- ▶ Hardware-Analysen
- ▶ Risiko- und Bedrohungsanalysen
- ▶ Reviews von Steuergeräte- und Bordnetzarchitekturen

## Unsere Kompetenzen

### Fahrzeug-Buskommunikation



- ▶ CAN, LIN, FlexRay
- ▶ Automotive Ethernet, DoIP

### Funkkommunikation



- ▶ Short Range: Wifi, Bluetooth, NFC, proprietäre Protokolle
- ▶ Long Range: GSM, Mobilfunk

### Smartphone App Security



- ▶ iOS
- ▶ Android

## Was macht die secunet Leistungen so besonders?

### ▶ Herstellerneutrale Analysen

frei von fachlichen Abhängigkeiten

### ▶ Individuelle Test-Szenarien

von der Betrachtung einzelner Steuergeräte bis hin zu Gesamtfahrzeuganalysen

### ▶ Ganzheitliche Kompetenz

vom Steuergerät über die Kommunikation bis zum Backend

### ▶ Datensicherheit und Vertraulichkeit

durch unsere festangestellten Mitarbeiter(innen) und einer für Hochsicherheit freigegebenen Infrastruktur

### ▶ Langjährige Erfahrung

im Umfeld der Automotive Security und in der Absicherung von vernetzten Fahrzeugen