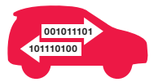
Our Experience is Your Advantage – the Automotive Division

Through numerous projects, our experts have gained valuable experience in the field of automotive security, which is why secunet's Automotive division covers a broad spectrum of topics.

In-vehicle security

- Component protection
- Vehicle immobiliser systems
- Secure flashing & coding
- Secure onboard communication

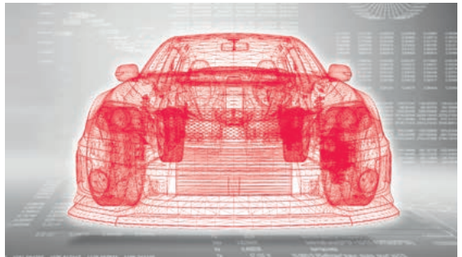
Secure vehicle communication



- Vehicle-to-grid
- Car-to-car communication
- Vehicle-to-infrastructure

Secure remote service integration

- Mobility services / car sharing
- Remote access & unlock
- Remote update service
- Online services & automotive cloud integration



secunet

secunet Security Networks AG
Kurfürstenstrasse 58
45138 Essen, Germany

www.secunet.com

Division Automotive Security
Konrad-Zuse-Platz 2
81829 Munich, Germany
Phone +49 (0) 201 5454 2502
automotive.security@secunet.com

Penetration Tests Automotive

Professional security assessments

secunet

Penetration tests to identify in-vehicle vulnerabilities

The digitalisation and connectivity of modern vehicles increasingly put both driver and vehicle at risk of cyber-attacks. At the same time, the constant growth in the complexity of in-vehicle networks increases the danger of attacks being successful and hinders the identification of potential vulnerabilities and error sources.

One proven technique to analyse security mechanisms is penetration testing. Here, testing is not based on functionality, but rather takes a systematic, step-by-step approach to investigating vectors of attack in control units and in-vehicle networks. Identified vulnerabilities are then evaluated in terms of their feasibility and potential impact, and countermeasures are specified.

With a laboratory fitted with high-grade equipment and a dedicated testing space for vehicles, secunet offers a wide and manufacturer-agnostic range of tests to analyse the security of networked vehicle systems, ranging from the individual control unit to the vehicle system as a whole.

Our range of services

- Robustness testing of protocol implementations, fuzz testing
- Logical attacks, white hat hacking
- Reverse engineering
- Source code analyses
- Hardware analyses
- Risk and threat analyses
- Reviews of control unit and onboard network architectures

Our expertise

In-vehicle bus communication

- CAN, LIN, FlexRay
- Automotive Ethernet, DoIP

Wireless communication

- Short range: Wi-Fi, Bluetooth, NFC, proprietary protocols
- Long range: GSM, mobile communication

Smartphone app security

- iOS
- Android

What makes secunet's services so special?

- **Manufacturer-independent analyses**
  Without third party influences
- **Tailored test scenarios**
  From investigations of individual control units to analyses of entire vehicles
- **All-encompassing expertise**
  Ranging from control units to communication with backend systems
- **Data security and confidentiality**
  Thanks to our internal team, and an infrastructure approved for high-level security
- **Many years of experience**
  In the field of automotive security and in the protection of networked vehicles