IOActive™

Hardware | Software | Wetware

SECURITY SERVICES

Vehicle Security Services Prepare for the future now

Driving Change

In-vehicle technology is a top selling point for today's car buyers. These connected systems provide measurable benefits to consumers and manufacturers–however, they also create opportunities to turn connected vehicles into targets for malicious cyber activity. It is imperative that automotive manufacturers take action now to infuse security into their vehicles and mitigate potential threats.

THE CONNECTED VEHICLE

Consumers assume modern vehicles will act as a natural extension of their digital environment, while simultaneously expecting greater safety, smarter navigation, and more accurate fault diagnostics. Vehicles can no longer exist as isolated instances of electromechanical engineering. They must link to a wider network of external systems to create a safer, more efficient, and more intelligent transportation system.

SECURITY BLIND SPOT

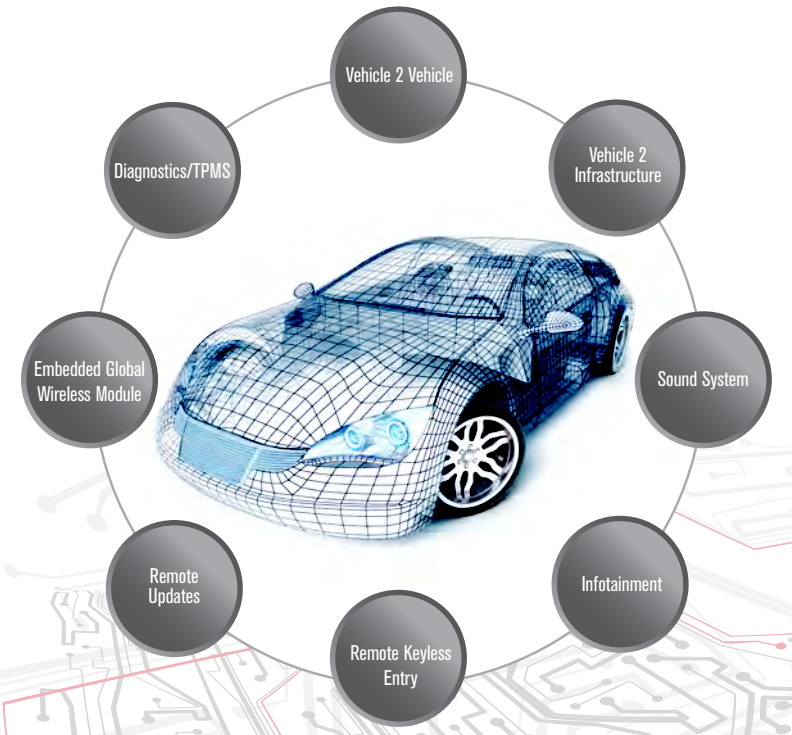
The current security model for vehicle control systems is designed to offer protection against the safety risks posed by electromechanical engineering faults. With the integration of Bluetooth and WiFi, the next generation of in-vehicle systems will process data from more than two dozen control units or sensors and provide access to radio functionality, toll payments, insurance data, the Internet, and social networks. The range of services will continue to broaden as automakers strive to keep pace with customer demands.

These services and systems rely on a constant stream of data flowing between the vehicle and external networks. If this vital link is not secured, a sophisticated cyber attacker can exploit it for malicious purposes.

In addition to consumer data privacy and physical safety concerns, smart vehicles must also defend against external system compromises. All networks share a certain level of trust; a breach of one vehicle may allow malicious attackers to gain access to all connected systems, including the manufacturer's own network. From there, they have the potential to affect not just one vehicle, but an entire fleet.

SECURITY BY DESIGN

With over 60 microprocessors and more than 10 million lines of software code, the connected vehicle relies on a plethora of cyber-physical systems and components to safeguard drivers. If a cyber attack can tamper with these systems, then the reliability and



safety of the vehicle will be compromised. Working with a security company with expertise in hardware, software, wireless, network, and embedded system attacks is critical. IOActive offers:

- Electronic Control Unit (ECU) testing (single purpose, multi-purpose, gateway, infotainment, telematics, and more)
- Software testing (diagnostic and maintenance tools, in-vehicle apps, PII enumeration, and more)
- Full vehicle assessments
- Customized research

RESEARCH DRIVEN SERVICES

IOActive is the leading connected vehicle security firm. We have invested heavily in primary research and work with top vehicle OEMs to understand the risks, threats, and business impacts facing the automotive industry. Our pioneering research has resulted in numerous studies and open source tools that have created awareness and armed manufacturers with the information they need to tackle their toughest security challenges.

IOActive leverages this body of research to provide clients with deeper assessments and superior guidance on leveraging innovative new technologies, while developing safer and more secure vehicles. We engage with product teams throughout the development lifecycle to ensure a security focus at every step.

COMPLETE COVERAGE

Our unique chip-to-code assessments provide a detailed security evaluation from semiconductors to software—for any component within the connected vehicle ecosystem. IOActive's hardware lab is equipped with Scanning Electron Microscopes (SEMs), Focussed Ion Beams (FIBs), confocal optical imaging equipment, and a variety of analytical tools. Our lab offers:

- Embedded device security analysis
- Physical attack resistance
- Low-level device firmware and driver assessment
- Chip and semiconductor analysis

Prepare for the Future Now

Leading automotive companies trust IOActive because:

- We conduct innovative research that enhances our automotive services
- We are trusted advisors who think like attackers—a unique mindset that enables us to stay ahead of motivated and sophisticated attackers
- We have a dedicated hardware engineering lab to assist in securing clients from chip-to-code
- We are highly skilled security professionals with real-world expertise in hardware, software, and wetware

For more information about IOActive's Vehicle Security Services, email info@ioactive.com or visit **www.ioactive.com**

ABOUT IOACTIVE

IOActive is the only global security consulting company delivering chip-to-code assessments, helping our clients stay ahead of tomorrow's threats—today. Grounded in cutting-edge research, we provide deep insights across hardware, software, and wetware security. As trusted strategic advisors to the Global 100, we help clients weave advanced security strategies throughout their products, services, and organizations.

IOActive™