IOActive.
Research-fueled Security Services

Vehicle Cybersecurity Services: Connected Vehicles and Beyond

Driving Change

In-vehicle technology is a top selling point for today's car buyers. What was once just a connected vehicle is now increasingly feature-rich from hybrid fuel vehicles and software systems like self-driving and Advanced Driver Assist Systems (ADAS) to other communication and integration options with artificial intelligence and machine learning. All this exciting technology, more than ever, turns modern vehicles into targets for malicious cyber activity. Automotive manufacturers must act now to infuse cybersecurity into their vehicles and mitigate potential threats.

The Software-Defined Vehicle (SDV)

Consumers assume SDV 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 now link to a wider network of external systems to create a safer and more efficient transportation system.

Cybersecurity Threatscape: Changing

Automotive cybersecurity models have evolved over time to include the concerns of connected vehicles. The threatscape is still changing; with the wide consumer adoption of electric vehicles and the integration of V2X communication, AI services and driverless technology, the next generation of in-vehicle systems will process data from an unprecedented number of external sources. 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 cyberattacker can exploit it for malicious purposes.

The increased sophistication of automotive vehicles provided by OEMs, in addition to components provided by Tier 1 and other suppliers, provides an ever-expanding attack surface. Current and new regulations, such as ISO/SAE 21434 and R155/156, must be considered for industry compliance.

In addition to regulations, consumer data privacy, and physical safety concerns, intelligent vehicles must also defend against external system compromises. Most 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.

Over a Decade of Vehicle Cybersecurity Research

IOActive has been a pioneer in vehicle cybersecurity research since 2013, including the ground-breaking Jeep hack that evolved into further vehicle research in commercial trucks, electric vehicle supply equipment (EVSEs), and autonomous vehicles.

Ground Vehicle Sectors/Years	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Automotive	■	■	■	■	■	■	■	■	■	■	■	■
Commerical Truck						■	■	■	■	■	■	■
EVSE Chargers						■	■	■	■	■	■	■
Autonomous Vehicles/ADAS										■	■	■

Cybersecurity at Phases of the Lifecycle

With all this new technology in place, the development of each component continues to follow an implementation lifecycle, including cybersecurity activities at each phase. Working with a cybersecurity company with expertise in hardware, software, wireless, network, and embedded system attacks is critical. IOActive's extensive automotive expertise provides a unique opportunity for partnerships with product teams throughout the development lifecycle to tackle their toughest cybersecurity challenges.

Requirements

- Expertise in current and emerging compliance regulations

Design

- Threat Analysis and Risk Assessment (TARA) Services
- Cybersecurity Component Design Review

Implementation

- Advanced ECU security testing with fault injection
- EV to Electric Vehicle Supply Equipment cybersecurity assessments
- Vehicle communication, V2X, and security testing, including GPS, WiFi, Bluetooth, cellular, and RF protocols
- AI/ML Security Assessments
- Code review and reverse engineering

Pre/Post Production

- Full vehicle testing
- Physical attack resistance
- Silicon security services
- Customized research

IOActive.

Research-Driven Services

IOActive is the leading connected vehicle cybersecurity firm. We have invested heavily in primary research and worked 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 tools that have created awareness and armed manufacturers with the information they need to be on the cutting edge of the latest attacks.

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.

RELATED RESEARCH

- NFC Relay Attack on TESLA Model Y
- Commonalities in Vehicle Vulnerabilities
- Uncovering Unencrypted Car Data in BMW Connected App
- Remote Exploitation of Unaltered Passenger Vehicle (the Jeep hack)

For more information about IOActive's Vehicle Cybersecurity Services, email

info@ioactive.com or visit ioactive.com.

Prepare for the Future Now

Leading automotive companies trust IOActive because:

1. **Pioneering Security Research:** IOActive is renowned for groundbreaking security research, uncovering vulnerabilities that shape industry standards and enhance global security protocols.
2. **Expert Vulnerability Assessments:** With deep expertise in comprehensive vulnerability assessments, IOActive identifies and mitigates risks that others might miss, ensuring robust protection for your infrastructure.
3. **Customized Security Solutions:** Tailoring their approach to each client's unique challenges, IOActive delivers personalized security strategies that address specific business needs and threats.
4. **Global Industry Recognition:** Acknowledged by peers and clients alike, IOActive's contributions to cybersecurity have earned them a prestigious position in the security community.
5. **Innovative Security Tools:** Leveraging state-of-the-art tools and techniques, IOActive stays at the forefront of security technology, offering cutting-edge solutions to modern threats.
6. **Dedicated Client Partnership:** IOActive prioritizes long-term relationships with their clients, offering continuous support and strategic guidance to navigate the evolving security threatscape.

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2024

SC MEDIA AWARDS

2 of 3 Most Important Researchers of the Last 30 years

One of the Most Important Cybersecurity Companies of the Last 30 years

REBOOT 19 SC Media Reboot Leadership Awards

ABOUT IOACTIVE

IOActive is a trusted partner for Global 1000 enterprises, providing research-fueled security services across all industries. Our cutting-edge security teams provide highly specialized technical and programmatic services including full stack penetration testing, program efficacy assessments and hardware hacking. IOActive brings a unique attacker's perspective to every client engagement to maximize security investments and improve clients' overall security posture and business resiliency.