Engineering Better Outcomes

Belcan

Case Study

Electronic Control Unit (ECU) Penetration Testing for a Major Automotive Supplier

Customer Overview

The customer is a top 20, tier 1 global automotive supplier of technology for autonomous driving and advanced driver assistance systems (ADAS) that facilitate secure connectivity and vehicle electrification. They engaged Belcan to assist in defining and executing a penetration testing program for an ECU with an application in the vision systems domain.

Customer Challenge

Rapid cybersecurity changes in the automotive industry have made securing embedded systems a much more complicated proposition than in the past. The customer's specific needs added complexity:

- Necessity to secure systems intended for the sale of more than 1.5 million vehicles across multiple original equipment manufacturers (OEMs) worldwide
- International manufacturing footprint with multiple plants
- Undocumented pre-existing testing equipment
- Safety-critical systems requiring customized assessment

ECU breaches can pose physical danger to end users – and significant liability risk for the supplier's customers – which is why the customer needed a skilled partner to define and perform penetration testing to meet all safety and quality criteria.

Belcan Solution

Belcan's embedded software engineering team performs full lifecycle development and is uniquely positioned to understand and address the details of cyber threats to embedded systems, including how these threats differ from traditional information systems security applications. Our specialized expertise allowed us to quickly begin work within the customer's ecosystem and deliver optimal outcomes at a much lower cost.

Our developers worked to customize and document an entirely new testing process with the customer's existing tools that was designed to be easily replicated. Penetration testing protocols were crafted to suit each embedded system type and its level of vulnerability and criticality, requiring direct input and approval from the OEM.

1/
Established
Penetration Testing Plan

2/
Developed
Test Environment

3/
Created
Attack Feasibility Matrix

4/
Executed
Penetration Testing

5/
Delivered
Penetration Testing Report

Project Outcome

Following a short ramp up phase and thorough testing, Belcan delivered a complete penetration report addressing the overall product cybersecurity ecosystem. This report identified:

- Vulnerabilities that can lead to compromise of ECU security
- Different severities of risks that can be used adversely against the ECU if exploited
- Recommendations that can fix these risks according to severity

Finished **ahead of schedule** by **9 months**

Project completed in **only 3 months**

Results delivered at **50% lower cost** than competing specialists

Belcan Difference

Belcan offers a breadth of qualified in-house resources unmatched in the industry, as well as a proven track record of cybersecurity expertise. Our teams include embedded software developers with extensive software interface experience, electrical engineers with a strong foundation in hardware devices and firmware, and verification engineers with experience analyzing, testing, and demonstrating vulnerabilities within complex systems. These experts are accustomed to working on safety-critical systems, quickly identifying requirements and executing testing that addresses potential security issues.

Belcan experts ramp up quickly, completing projects at the highest levels of quality and providing ongoing cybersecurity verification support and regression testing as needed, at a significant cost savings. Projects recently completed for similar customers include:

- A white box approach for an embedded vehicle control system with several interfaces, including CAN, 100BASE-TX, RS-485, discrete I/O, and field-loadable software
- Security vulnerability assessments and black-box penetration testing on an IP-based vehicle control unit responsible for on- and off-vehicle communications, including remote data loading
- Design and testing of an RF Skimmer interceptor, including design of a 16 layer PCB with Atom Intel Processor, Max10 FPGA and ten software defined ratios

See how Belcan's integrated and adaptive engineering services can work for you.

Contact Us

Belcan