Automotive, IoT and Embedded Pentesting Success Stories

Why You Should Choose Embitel

Scope and Our Approach

Automotive and embedded platforms operate within tightly coupled, multi-layered architectures. Security failures often emerge at trust boundaries, where firmware, middleware, hypervisors, and connected services intersect.

Our expertise spans firmware, ECU architectures, communication stacks, secure boot chains, hypervisors, Trusted Applications, and connected ecosystems.

Case Study 1

Hypervisor Domain Isolation Assessment

A gateway ECU running multiple isolated domains required validation of partition integrity and resistance to lateral movement.

Our Solution

We analysed inter-domain communication surfaces, uncovered information disclosure vectors, and chained findings with privilege escalation paths to simulate cross-partition compromise.

Outcomes:

- Identified cross-domain escalation paths during development
- Strengthened partition isolation before production
- Reduced systemic risk across hosted vehicle functions

Case Study 2

Trusted Execution Environment (OP-TEE) Security Review

A Trusted Execution Environment handling sensitive cryptographic operations required deep architectural and implementation review.

Our Solution

We performed secure code review and architectural analysis of Trusted Applications, evaluating cryptographic handling, memory isolation, and privilege enforcement.

Outcomes:

Identified critical design weaknesses before deployment

Redefined cryptographic trust boundaries

Eliminated systemic risk prior to integration

Case Study 3

In-Vehicle Infotainment Penetration Testing

A connected infotainment platform required offensive validation before release. The objective was to identify potential attack vectors that may later compromise the system.

Our Solution

We assessed exposed services, persistence mechanisms, remote access vectors, and denial-of-service resilience across system layers.

Outcomes:

- Identified high-impact vulnerabilities pre-release
- Reduced attack surface across connected components
- Improved resilience against remote compromise

Case Study 4

Real-Time TLS & Certificate Validation Assessment

A connected automotive component relied on time-sensitive certificate validation logic to maintain trust integrity.

Our Solution

We developed custom tooling to intercept and analyse TLS traffic, evaluate certificate lifecycle handling, and test validation logic under adversarial timing conditions.

Outcomes:

- Identified and mitigated timing-based trust inconsistencies
- Strengthened cryptographic communication
- Preserved production-grade trust models

Contact Us

Email

sales@embitel.com

Website

www.embitel.com

Location

India, Germany,

USA, UK, UAE