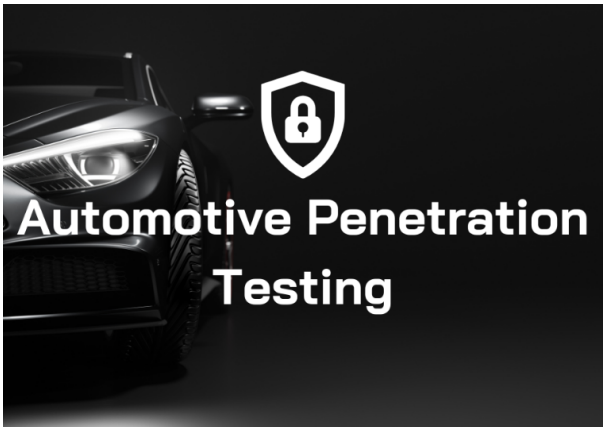
Contact us

Automotive Penetration Testing



What Is Automotive ECUs Penetration Testing?

Automotive ECUs Penetration Testing is a specialized cybersecurity process aimed at identifying potential vulnerabilities within an **Electronic Control Unit (ECU)**. By simulating hacking attempts on vehicle components, this method exposes weaknesses in a controlled environment, focusing exclusively on the target ECU.

Our cybersecurity experts perform these tests at **Applus+ Laboratories' global facilities** or on-site at client locations. The outcome is an **Evaluation Technical Report (ETR)** that documents vulnerabilities and includes detailed instructions for replicating the tests, ensuring reproducibility and reliability.

Why Is Automotive ECUs Penetration Testing Important?

Penetration Testing is a critical component of modern vehicle cybersecurity. It identifies and addresses vulnerabilities, enhancing the **functional safety and security** of vehicles while protecting road users from potential threats.

The Role of Penetration Testing

Penetration Testing evaluates the effectiveness of implemented security measures and uncovers undetected vulnerabilities. The testing approach varies by **scope**:

- **Black-box testing:** Simulates real-world attacks without prior knowledge of the system, providing a broader perspective with less depth.
- **White-box testing:** Involves in-depth analysis using comprehensive system knowledge, allowing for detailed and thorough testing.

The Increasing Complexity of Modern Automotive Systems

Contemporary vehicles often contain over **50 ECUs** and as many as **100 million lines of code**. This complexity, combined with the rise of **smart vehicles** and expanded communication interfaces, creates a broader attack surface, necessitating robust **cybersecurity measures**.

Integrating Security into the Development Lifecycle

To mitigate cybersecurity risks, it is essential to embed **security practices** into every phase of the vehicle development lifecycle. Early incorporation of **secure-by-design principles** helps reduce vulnerabilities before production begins.

Adopting International Standards for Cybersecurity

The automotive industry increasingly aligns with standards like **ISO/SAE 21434** to manage cybersecurity risks effectively. These frameworks promote **proactive security measures** and emphasize the importance of validating implemented solutions to identify **residual risks**.

What Are the Risks and Cybersecurity Requirements for Automotive ECUs?

To understand and address the risks associated with automotive ECUs, it is vital to recognize the **challenges and methodologies** involved. **Penetration Testing** bridges the gap between theoretical standards and practical cybersecurity applications.

- **Challenges in Complying with Cybersecurity Standards:** Understanding and interpreting cybersecurity standards can be challenging, as some requirements lack clarity. This ambiguity allows organizations flexibility in tailoring their processes but also demands a deep understanding to ensure compliance.
- **Risks in the Automotive Industry:** Automotive risks primarily include safety impacts (e.g., Functional Safety and ISO 26262) and threats to road users (e.g., pedestrians and cyclists). These risks can result in safety, financial, operational, and privacy consequences.
- **Addressing Risks Through Penetration Testing:** Penetration Testing evaluates whether cybersecurity goals, such as the CIAA quartet of protection, are achieved for each asset. It also identifies previously undetected vulnerabilities and attack scenarios.

What Are the Regulations and International Standards for Automotive ECUs?

Understanding and adhering to regulations governing automotive ECUs is crucial for ensuring **compliance** and addressing **cybersecurity vulnerabilities**. These frameworks provide clear **guidelines for managing risks** and aligning **testing methodologies** with industry standards.

Global Market

- **UN Regulation No. 155 (R155):** A United Nations regulation focused on road vehicle cybersecurity, primarily targeting OEMs. It includes comprehensive threat scenarios, vulnerabilities, and mitigation strategies, serving as a valuable reference for the supply chain.
- **ISO/SAE 21434:2021:** An international standard that establishes a framework for developing and maintaining a Cybersecurity Management System. It details methodologies for conducting TARA (Threat Analysis and Risk Assessment) activities.

Chinese Local Market

- **GB-44495:** China's equivalent to UN Regulation R155, featuring more specific requirements. This regulation mandates penetration testing at the vehicle level and will become mandatory for all vehicles sold in China starting January 2026.

Why Choose Applus+ Laboratories for Penetration Testing?

Applus+ Laboratories provides specialized penetration testing services tailored to the automotive supply chain. Our approach aligns with global and local regulations, offering the following benefits:

- **Trust**
- **Regulatory Compliance**
- **Market Compliance**
- **Risk Reduction**

Clients rely on our expertise as an independent third-party laboratory to ensure accurate and reliable penetration testing.

Independent Cybersecurity Penetration Testing for the Global Market

For clients targeting **international markets**, our **penetration testing methodology** considers the unique **technologies**, **functionalities**, **complexities**, and **safety requirements** of the components. We recommend **grey-box** and **white-box evaluations** to verify the effectiveness of **cybersecurity measures** and identify remaining **vulnerabilities**.

Testing Methodology and Best Practices

Our methodology at Applus+ Laboratories is structured into the following stages:

1. **Discovery and Proving:** Initial identification of system features and potential vulnerabilities.
2. **Enumeration:** Cataloging system components and their potential attack vectors.
3. **Vulnerability Assessment:** Evaluating the likelihood and impact of identified vulnerabilities.
4. **Penetration Testing Plan Definition:** Designing a comprehensive and tailored testing strategy.
5. **Penetration Testing Execution:** Conducting the actual penetration tests according to the defined plan.
6. **Reporting:** Delivering a detailed Evaluation Technical Report (ETR) with findings and recommendations.

By choosing Applus+ Laboratories, clients gain access to **cutting-edge testing methodologies** and a team of **seasoned cybersecurity professionals** dedicated to enhancing the **safety and security** of automotive systems.