Automotive Cybersecurity and CAN Bus Hacking Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The modern vehicle is a Software-Defined Vehicle, transforming from a mechanical machine into a complex, interconnected cyber-physical system. This rapid evolution, driven by features like Advanced Driver-Assistance Systems, Vehicle-to-Everything communication, and Autonomous Driving, has dramatically expanded the Attack Surface. The core of in-vehicle communication, the Controller Area Network, was designed decades ago without inherent security mechanisms like authentication or encryption, making it a critical Vulnerability.

Automotive Cybersecurity and CAN Bus Hacking Training Course is an essential deep dive into Vehicle Hacking and In-Vehicle Network Security, equipping professionals with the practical skills to defend modern automobiles. Participants will master the methodologies of a Threat Actor by conducting Ethical Hacking and CAN Bus Reverse Engineering on real-world vehicle architectures. The curriculum is meticulously crafted to cover both offensive and defensive techniques, focusing on hands-on application of Penetration Testing tools and compliance with emerging global standards like ISO/SAE 21434 and UN Regulation No. 155, ensuring readiness for the future of Secure Mobility.

Programme Curriculum

Automotive Cybersecurity and CAN Bus Hacking Training Course

Introduction

The modern vehicle is a Software-Defined Vehicle, transforming from a mechanical machine into a complex, interconnected cyber-physical system. This rapid evolution, driven by features like Advanced Driver-Assistance Systems, Vehicle-to-Everything communication, and Autonomous Driving, has dramatically expanded the Attack Surface. The core of in-vehicle communication, the Controller Area Network, was designed decades ago without inherent security mechanisms like authentication or encryption, making it a critical Vulnerability.

Automotive Cybersecurity and CAN Bus Hacking Training Course is an essential deep dive into Vehicle Hacking and In-Vehicle Network Security, equipping professionals with the practical skills to defend modern automobiles. Participants will master the methodologies of a Threat Actor by conducting Ethical Hacking and CAN Bus Reverse Engineering on real-world vehicle architectures. The curriculum is meticulously crafted to cover both offensive and defensive techniques, focusing on hands-on application of Penetration Testing tools and compliance with emerging global standards like ISO/SAE 21434 and UN Regulation No. 155, ensuring readiness for the future of Secure Mobility.

Course Duration

5 days

Course Objectives

1. Understand the Automotive Threat Landscape and the evolution of Vehicle-to-Cloud security.
2. Analyze the technical specifications and inherent CAN Bus Vulnerabilities of the Controller Area Network
3. Perform CAN Bus Reverse Engineering to identify, interpret, and manipulate critical vehicle messages.
4. Execute hands-on In-Vehicle Network Penetration Testing using industry-standard tools and frameworks.
5. Develop robust Intrusion Detection Systems and Intrusion Prevention Systems for IVNs.
6. Assess and mitigate vulnerabilities in other automotive protocols like LIN, FlexRay, and Automotive Ethernet.
7. Apply Threat Analysis and Risk Assessment methodologies specific to automotive systems.
8. Implement Secure Boot and Hardware Security Modules for ECU Security.
9. Master the principles of Automotive Software Security and secure coding practices.
10. Comply with the mandatory UN R155 and ISO/SAE 21434 standards.
11. Simulate and defend against common remote and physical Car Hacking attack vectors.
12. Explore security challenges related to V2X Communication and Autonomous Driving systems.
13. Create an effective Cybersecurity Incident Response plan for connected vehicles.

Target Audience

1. Automotive Cybersecurity Engineers
2. Embedded Systems Engineers / ECU Developers
3. Penetration Testers and Security Researchers transitioning to automotive.
4. Automotive Network Architects and Design Engineers
5. Cybersecurity Managers responsible for UN R155 compliance.
6. Quality Assurance and Validation Engineers in automotive.
7. IT/Cybersecurity Professionals interested in Connected Car technology.
8. Forensics and Incident Response Teams in the transportation sector.

Course Modules

Module 1: Automotive Network Fundamentals and Attack Surface Mapping

- Arbitration, message ID, data field, and error handling.
- Introduction to LIN, FlexRay, and Automotive Ethernet.
- Understanding the domain and zonal controller layout.
- Identifying remote and physical access points
- Case Study: The Jeep Cherokee Remote Attack analysis of how a remote vulnerability led to CAN bus manipulation.

Module 2: CAN Bus Reverse Engineering and Message Analysis

- Working with CAN interfaces, tools like CANtact or Vector CANalyzer.
- Techniques for passively collecting CAN traffic.
- Using statistical methods and brute-forcing to identify signals
- Generating malicious messages to test system stability.
- Case Study: Reverse-engineering a vehicle's door lock/unlock command by correlating physical actions with CAN message changes.

Module 3: Active CAN Bus Hacking and Manipulation

- Message Spoofing
- Bus-Off Attacks.
- Diagnostic Protocols Hacking.
- ECU Reprogramming.
- Case Study: Simulating a "ghost braking" or "steering manipulation" attack by injecting high-priority CAN frame.

Module 4: Defensive Coding and ECU Security

- Secure Coding for Embedded Systems.
- Cryptography in Automotive.
- Hardware Security
- Secure Boot & Secure Flashing.
- Case Study: Analysis of a supply chain attack where malicious code was introduced during the manufacturing process.

Module 5: Cybersecurity Standards and Regulation Compliance

- Deep dive into the standard for Cybersecurity Engineering.
- Implementing a Cybersecurity Management System.
- Threat Analysis and Risk Assessment.
- Integrating security activities throughout the product lifecycle.
- Case Study: Developing a CSMS framework for a new vehicle platform to meet UN R155 type approval requirements.

Module 6: Intrusion Detection and Prevention Systems (IDS/IPS)

- Techniques for real-time traffic analysis.
- Statistical and machine learning methods for identifying malicious CAN traffic patterns.
- Programming simple rule-sets for known attack signatures.
- Firewall Implementation.
- Case Study: Building and testing a simple CAN IDS that detects a spoofed message attack in a live lab environment.

Module 7: Connected and Autonomous Vehicle (CAV) Security

- V2X Communication Security.
- Telematics and Remote Update Security.
- Infotainment (IVI) and App Security.
- Autonomous Driving Sensor Security.

- Case Study: Analyzing a vulnerability in an OTA update mechanism and developing a secure update protocol.

Module 8: Incident Response and Post-Exploitation Forensics

- Incident Response Planning.
- Digital Forensics in Automotive.
- Post-Incident Analysis.
- Legal and Ethical Considerations.
- Case Study: Conducting a simulated forensic investigation on a vehicle's log data after a successful CAN bus hack to determine the entry point and exploit.

Training Methodology

This course employs an intensive **hands-on, practical-led** methodology:

- Instructor-Led Sessions.
- Live Demonstrations.
- Practical Labs.
- Case Study Analysis.
- Defense Development Workshops.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com