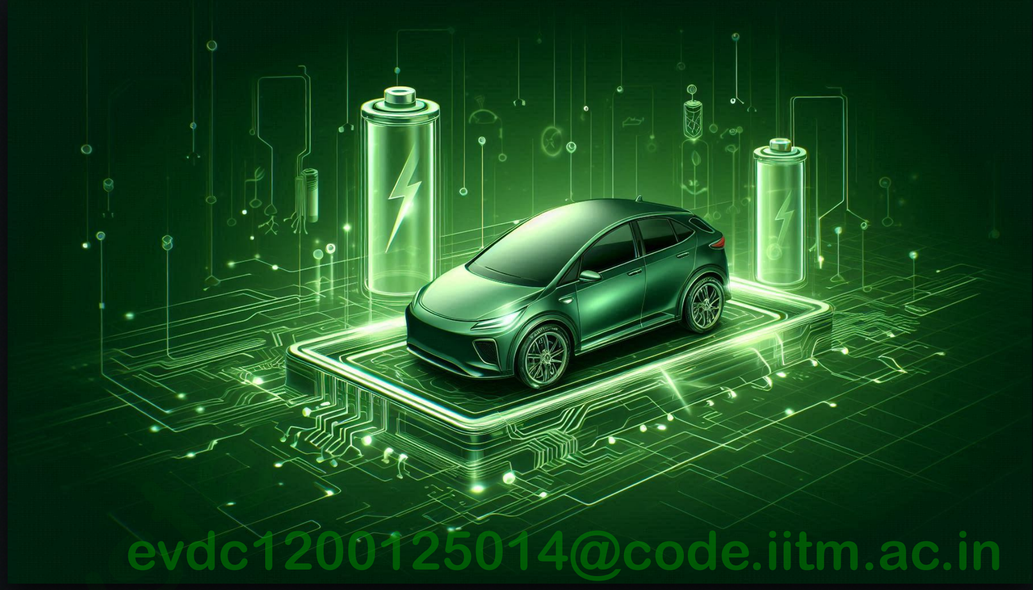


Automotive Cybersecurity

Electric Vehicle Engineering & Software Development

Sudarshana Karkala

EV.Engineer, AI-Driven Battery Safety

Electric Vehicle Engineering & Development, CODE, IIT Madras

✆ +91 9845561518 | ✉ carsoftwaresystems @ gmail.com | carsoftwaresystems.com

Course overview

This course provides a comprehensive understanding of cybersecurity in the automotive industry. With a focus on practical applications, hands-on exercises, and real-world case studies, participants will gain the necessary skills to identify, mitigate, and prevent cyber threats in modern vehicles.

- Introduction to Automotive Cybersecurity
- Cybersecurity Basics
- Secure Boot & Secure Firmware Updates
- Secure Gateway & Network Security
- Infrastructure Protection & Intrusion Detection
- Cybersecurity in OTA Updates
- Real-World Attack Scenarios & Penetration Testing
- Case Studies & Advanced Topics
- Final Assessment & Project Work

1. Introduction to Automotive Cybersecurity

- Understanding Automotive Security
  - Importance of cybersecurity in modern vehicles
  - Cybersecurity challenges in connected and autonomous vehicles
- Attack Surfaces in Modern Vehicles
  - ECUs, CAN Bus, Telematics, V2X, Infotainment systems
- Cybersecurity Regulations & Compliance
  - ISO 21434, UNECE WP.29, ASPICE
- Real-World Case Studies
  - Jeep Cherokee Hack, Tesla Key Fob Hack, Nissan Leaf vulnerability
- Hands-on Lab
  - Exploring Cybersecurity Attack Vectors in a Simulator

2. Cybersecurity Basics

- Cryptography Basics
  - AES, RSA, ECC, HMAC
- Secure Communication in Vehicles
  - CAN, LIN, FlexRay, Automotive Ethernet
- Authentication & Access Control in Vehicles
  - Digital signatures, message authentication
- Common Attack Techniques
  - Spoofing, Replay attacks, DoS attacks
- Hands-on Lab
  - Sniffing and Analysing CAN Bus Traffic using an Online Simulator

3. Secure Boot & Secure Firmware Updates

- What is Secure Boot?
  - Ensuring boot loader security
- Secure Boot Implementation in ECUs
  - Trusted execution environments (TEE)
- Firmware Update Security
  - Code Signing & Integrity Checks
- Practical Attacks on Firmware
  - Firmware Tampering & Bypass Techniques
- Hands-on Lab
  - Analysing Firmware Signing & Validation in a Virtual Environment

4. Secure Gateway & Network Security

- Introduction to Secure Gateways
  - Role of secure gateways in SDVs
- Firewall & Intrusion Prevention in Automotive Networks
- Attack Scenarios in Automotive Networks
  - Man-in-the-Middle (MITM) & Packet Injection Attacks
- Defensive Mechanisms & Cryptographic Controls
- Hands-on Lab
  - Simulating & Detecting Intrusions in an Automotive Network

5. Infrastructure Protection & Intrusion Detection

- Intrusion Detection Systems (IDS) in Vehicles
- Threat Modelling & Risk Assessment for Automotive Systems
- Anomaly Detection with AI & ML
- Cloud-Based Security Solutions for Connected Vehicles
- Hands-on Lab
    - Detecting Cyber Threats in a Simulated Automotive IDS

6. Cybersecurity in OTA Updates

- Overview of Secure OTA Updates
- Firmware Integrity & Authentication Checks
- Attack Scenarios on OTA Systems
- Defensive Techniques in OTA Updates
- Hands-on Lab
    - Simulating Secure OTA Updates in a Cloud Environment

7. Real-World Attack Scenarios & Penetration Testing

- Wireless Attack Surfaces in Vehicles
  - Bluetooth, WiFi, Keyless Entry Exploits
- Pen-Testing Methodologies in Automotive Systems
- Fuzz Testing for CAN & Ethernet
- Reverse Engineering & Firmware Analysis
- Hands-on Lab
  - Pen testing an Automotive System using Open-Source Tools

8. Final Case Studies & Advanced Topics

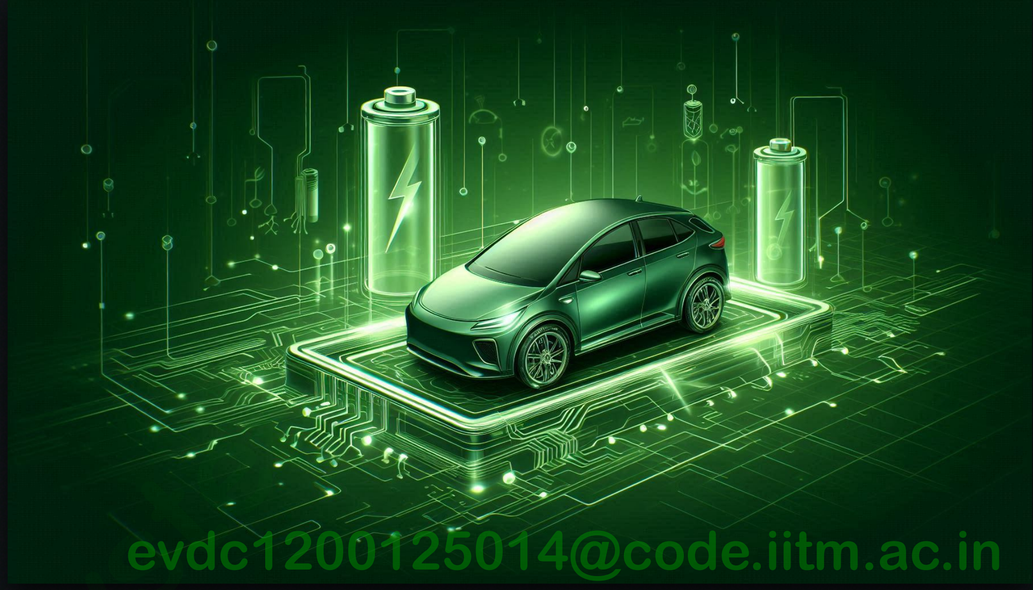
- Deep Dive: Tesla, Mercedes, Toyota Security Strategies
- AI in Automotive Cybersecurity
- Blockchain for Automotive Security
- Zero Trust Security for Connected Vehicles
- Hands-on Lab
    - Final Project : Simulating a Security Attack & Defence Strategy

Required Tools & Simulators

- **Wireshark** – Packet sniffing & CAN Bus Analysis
- **ICSim (CAN Bus Simulator)** – Hands-on CAN hacking & security
- **Scapy (Python-based tool)** – Simulating automotive attacks
- **Kali Linux on Mac (via Virtual Machine)** – Security testing & pen testing
- **Open-source OTA Testing Tools** – Secure OTA update simulations

Why This Course is Ideal for Professionals?

- **Hands-on Learning** – 50% practical work using online tools
- **Real-World Scenarios** – Industry case studies & simulations
- **No Extra Hardware Needed** – Everything runs on MacBook!
- **Job-Ready Skills** – Prepares professionals for Automotive Security roles



Thank you

Sudarshana Karkala

EV.Engineer, AI-Driven Battery Safety

Electric Vehicle Engineering & Development, CODE, IIT Madras

✆ +91 9845561518 | ✉ carsoftwaresystems @ gmail.com | carsoftwaresystems.com