VEHI QILLA

In-Vehicle Secure Architecture Course Outline

Area	Item & Schedule	Topics
Automotive Cybersecurity Basics	Why Automotive Cybersecurity **(4 hrs)**	• Transformation in Mobility • Connected and Autonomous Vehicles (CAV) • Vehicle Technologies • Cyber Challenges in CAVs • Recent Cyber Attacks on CAVs • Difference between IT and Automotive Cybersecurity
	Automotive Cybersecurity Basics **(4 hrs)**	• CIA • Authentication • Encryption • Cybersecurity elements of the Vehicle • Vehicle Connectivity • V2X Cybersecurity Challenges • Electric Vehicle Cybersecurity • Security By Design • Privacy & Tracking
System	Attack Vector @Vehicle Level **(4 hrs)**	• Third Party Apps • Key Fob Hacking • OBD II Hacking • Vehicle to vehicle • Vehicle to Infrastructure • Vehicle to Everything • Personal Data

	Communication buses/In-vehicle Networks **(4 hrs)**	• Assets inside Vehicle • In-Vehicle Communication • CANBus • SAE J1939 • Automotive Ethernet • Wi-Fi • Bluetooth • GSM
Software	How to Assess vulnerabilities of ECUs **(4 hrs)**	• Active Vehicle Vulnerability Analysis • Passive Vehicle Vulnerability Analysis • Supply Chain Vulnerability Analysis • Software Vulnerability Analysis • Key Cyber Attack Vectors in Automotive
	Cyber security algorithm in automotive **(2 hr)**	• Software Development in Automotive World • Cyber-Secure Implémentation and Prevention • Security By Design • Life Cycle Management Security Post-Production
	SW artifacts update over Air Protection **(2 hrs)**	• OTA (Over the Air Updates) • Entities involved in OTA updates • Technical Overview on remote software updates • Cybersecurity in OTA updates • Cybersecurity challenges in remote SW update
Verification	Hacking into an ECU live session **(4 hrs)**	• Pre-Engagement • Vehicle/ECU Intelligence Gathering • Automotive Threat Modeling • ECU Vulnerability Analysis • ECU Exploitation
	Different verification mechanisms - Penetration testing, Vulnerability testing etc	• Passive Vehicle Reconnaissance • Active Vehicle Reconnaissance

	(4 hrs)	- Whitebox Automotive Pen-Testing - Blackbox Automotive Pen-Testing
	Tools / Infrastructure needs **(4 hrs)**	- Scanning Tools - Wi-Fi Tools - Bluetooth Tools - Tools for GSM network - Purpose & Working of each Tools
	Live Demos & Exercises **(4 hrs)**	- Fleet Cyber Monitoring Live Demo - Collection of Vehicle Cybersecurity Logs Demo

Who Should Attend (Pre-requisite)

This training provides participants in the automotive industry with the necessary basic knowledge to be able to integrate cybersecurity in the development of any new Connected & Autonomous Vehicle.

This training is appropriate for

- Individuals who work in the automotive cybersecurity, management, engineering, or audit environment.
- Automotive Engineering Manager
- Automotive Product & Infrastructure
- Automotive embedded device & system engineers, designers, testers, manufacturers and suppliers
- Developers working with embedded systems
- Ethernet and CAN Bus Software Engineers and Testers
- Autonomous Vehicle Development Software and Hardware Engineers
- Automotive Verification and Validation Engineers and Managers