PiEST Systems

PIEST SYSTEMS (OPC) PRIVATE LIMITED

Automotive Cyber Security Syllabus

6-Month Course Syllabus

Week 1 – Introduction

- Cybersecurity basics – CIA triad, Threats vs Vulnerabilities vs Attacks
- Automotive Cybersecurity overview – ECU, Gateway, Telematics
- Standards: ISO/SAE 21434, UNECE WP.29 overview
- **Lab:** Identify attack surfaces in a modern vehicle

Week 2 – Cryptography Foundations

- Symmetric crypto (AES, DES, ChaCha20)
- Asymmetric crypto (RSA, ECC, EdDSA)
- Hash functions & MACs (SHA2, SHA3, HMAC)
- **Lab:** Implement AES encryption/decryption in C

Week 3 – Applied Cryptography in Automotive

- Digital signatures & certificates (PKI in cars)
- Key management in ECUs (key rotation, provisioning)
- Random Number Generators (TRNG vs PRNG)
- **Lab:** Generate & verify ECDSA signatures

Week 4 – Types of Security Hardware

- Secure elements:
  - HSM
  - SSM
  - TPM, TrustZone, Secure Element chips
- Automotive microcontrollers (NXP S32K, Infineon AURIX, STM32H7)
- **Lab:** Access crypto services via an HSM simulator

Phase 2 – Automotive Protocols & Secure Communication (Weeks 5–8)

Week 5 – In-Vehicle Networks & Attack Surfaces

- CAN, CAN FD, LIN, FlexRay, Automotive Ethernet
- UDS (ISO 14229) services & security access
- DoIP (ISO 13400) basics
- **Lab:** Capture & analyze CAN traffic with PCAN/SocketCAN

Week 6 – Attacks on Automotive Networks

- Replay, Fuzzing, Spoofing, DoS, Bus flooding
- Diagnostic security bypass (Seed/Key brute force)
- **Lab:** Perform replay attack on CAN bus demo

Week 7 – Secure Onboard Communication (SecOC)

- AUTOSAR SecOC architecture
- Freshness counter & MAC generation
- Synchronization challenges
- **Lab:** Implement SecOC protection on CAN

Week 8 – Secure Communication over IP

- TLS/DTLS in automotive Ethernet
- VPN, IPsec for backend–vehicle links
- Secure V2X communication (IEEE 1609.2)
- **Lab:** Setup secure TLS client/server for ECU simulator

Phase 3 – Secure ECU Software & Boot Process (Weeks 9–12)

Week 9 – Secure Boot Fundamentals

- Chain of Trust
- Signed firmware validation
- Anti-rollback
- **Lab:** Basic secure bootloader on STM32/S32K

Week 10 – Firmware Updates & OTA Security

- Secure flashing (local/OTA)
- Firmware integrity (hash/signature)
- Rollback protection
- **Lab:** Simulate OTA update with signature verification

Week 11 – Secure Memory & Runtime Protections

- MPU & TrustZone
- Code/data execution protection (XOM, secure regions)
- Anti-tamper & fault injection
- **Lab:** Configure TrustZone on Cortex-M33

Week 12 – Hardware Security Modules in Action

- Automotive HSM functions
- SSM vs HSM
- **Lab:** Implement seed/key challenge with HSM emulation

Phase 4 – Threat Modeling, Standards & Pen-Testing (Weeks 13–16)

Week 13 – Threat Modeling

- STRIDE, DFD, Attack Trees
- Example: Telematics ECU threat model
- **Lab:** Threat model for CAN-based ECU

Week 14 – ISO/SAE 21434 in Practice

- Cybersecurity goals, claims, work products
- Security V-model
- **Lab:** Create cybersecurity requirements for ECU

Week 15 – UNECE WP.29 & Compliance

- OEM & supplier regulatory requirements
- CSMS, SUMS
- **Lab:** Compliance checklist for ECU project

Week 16 – Penetration Testing & Tools

- ECU/IVN pentest methodology
- Tools: CANoe, Scapy, Wireshark, CANalyzer
- **Lab:** Fuzz a simulated UDS service

Phase 5 – Advanced Security (Weeks 17–20)

Week 17 – Intrusion Detection Systems (IDS)

- CAN anomaly detection
- Rule-based vs ML-based IDS
- **Lab:** Build IDS for CAN

Week 18 – Telematics & Cloud Security

- TCU attack vectors
- Secure MQTT, TLS
- **Lab:** Secure a telematics channel

Week 19 – V2X & Future Trends

- C-ITS, V2V, V2I
- IEEE 1609.2 PKI
- Quantum-safe crypto
- **Lab:** Sign & verify V2X messages

Week 20 – Case Studies

- Jeep Cherokee hack
- Tesla Model S hacks
- Bluetooth/TPMS vulnerabilities
- **Lab:** Analyze case & simulate simple exploit

Phase 6 – Capstone & Industry Prep (Weeks 21–24)

Week 21 – Secure Development Lifecycle

- Cybersecurity in ASPICE & AUTOSAR
- CI/CD with security checks
- **Lab:** Secure coding audit

Week 22 – Forensics & Incident Response

- Automotive logging strategies
- Post-attack workflow
- **Lab:** Extract attack traces from CAN logs

Week 23 – Final Capstone Project

Build a secure ECU with:

- Secure Boot
- HSM key storage
- SecOC CAN
- OTA with signature validation

Week 24 – Presentation & Industry Outlook

- Present capstone
- Trends: EV charging security, AV security, AI in IDS
- Career pathways

Deliverables

- Weekly assignments & labs
- **Mid-term project (Week 12):** Secure Boot + SecOC demo
- **Final capstone (Week 23–24):** Secure ECU subsystem + documentation

1 Month Crash Course (4 Weeks)

Week 1 – Cybersecurity & Automotive Basics

- Cybersecurity overview, CIA triad
- Automotive ECUs & in-vehicle networks (CAN, LIN, FlexRay, Ethernet)
- Attack surfaces in vehicles
- **Lab:** Capture & analyze CAN traffic using Wireshark/PCAN

Week 2 – Cryptography & Secure Communication

- Basics of AES, RSA, ECC
- Hashing algorithms (SHA2 / SHA3)
- Secure Onboard Communication (SecOC) overview

- UDS Security Access (Seed/Key)
- **Lab:** Implement simple AES encryption on CAN messages

Week 3 – ECU Security Foundations

- Secure Boot basics
- Firmware integrity validation
- OTA (Over-the-Air) update security basics
- **Lab:** Demonstration of Secure Boot validation flow

Week 4 – Case Studies & Compliance Intro

- Jeep Cherokee Hack
- Tesla Hack overview
- Introduction to ISO/SAE 21434
- **Lab:** Perform simple replay attack demo & mitigation

Outcome

✓ Quick automotive cybersecurity awareness
✓ Hands-on exposure to real attacks and security mechanisms