



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 in automotive:
 - **HSM (Hardware Security Module)**
 - **SSM (Secure Subsystem Module)**
 - TPM, TrustZone, SE chips
- ❖ Automotive microcontrollers with security IP (NXP S32K, Infineon AURIX, STM32H7)
- ❖ Lab: Accessing 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 and 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 a CAN bus demo

Week 7 – Secure Onboard Communication (SecOC)

- ❖ AUTOSAR SecOC architecture
- ❖ Freshness counter & MAC generation
- ❖ Challenges in synchronization
- ❖ Lab: Implement SecOC protection on CAN messages

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 in embedded systems
- ❖ Signed firmware validation
- ❖ Anti-rollback protection
- ❖ Lab: Implement a basic secure bootloader on STM32/S32K board

Week 10 – Firmware Updates & OTA Security

- ❖ Secure flashing (local vs OTA)
- ❖ Firmware integrity (hash/signature checks)
- ❖ Update rollback protection
- ❖ Lab: Simulate OTA update with signature verification

Week 11 – Secure Memory & Runtime Protections

- ❖ MPU (Memory Protection Unit) & TrustZone
- ❖ Code & data execution protection (XOM, Secure regions)
- ❖ Anti-tamper & fault injection protection
- ❖ Lab: Configure TrustZone partitions on Cortex-M33

Week 12 – Hardware Security Modules in Action

- ❖ Automotive HSM functions: crypto, key storage, secure boot
- ❖ SSM vs HSM usage scenarios
- ❖ Lab: Implement seed/key challenge with HSM emulation

Phase 4 – Threat Modeling, Standards & Penetration Testing (Weeks 13–16)**Week 13 – Threat Modeling**

- ❖ STRIDE, DFD, Attack Trees in automotive
- ❖ Practical examples: Telematics ECU threat model
- ❖ Lab: Build a threat model for a CAN-based ECU

Week 14 – ISO/SAE 21434 in Practice

- ❖ Cybersecurity goals, claims, work products
- ❖ Security V-model in development lifecycle
- ❖ Lab: Create cybersecurity requirements for an ECU

Week 15 – UNECE WP.29 & Compliance

- ❖ Regulatory requirements for OEMs & suppliers
- ❖ CSMS (Cyber Security Management System)
- ❖ SUMS (Software Update Management System)
- ❖ Lab: Draft compliance checklist for an ECU program

Week 16 – Penetration Testing & Tools

- ❖ Methodology for ECU/IVN pentesting
- ❖ Tools: CANoe, Scapy, Wireshark, CANalyzers
- ❖ Lab: Perform fuzzing on 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 a basic IDS to detect abnormal CAN traffic

Week 18 – Telematics & Cloud Security

- ❖ Attack vectors in TCU (Telematics Control Unit)
- ❖ Secure MQTT, TLS for backend connectivity
- ❖ Lab: Secure a simulated telematics channel

Week 19 – V2X & Future Trends

- ❖ C-ITS, V2V, V2I communication
- ❖ IEEE 1609.2 PKI for V2X
- ❖ Quantum-safe crypto for automotive
- ❖ Lab: Sign and verify V2X messages

Week 20 – Case Studies of Real Attacks

- ❖ Jeep Cherokee hack (Miller & Valasek)
- ❖ Tesla Model S hacking cases
- ❖ Bluetooth/TPMS vulnerabilities
- ❖ Lab: Analyze case study and simulate simple exploit

Phase 6 – Capstone & Industry Preparation (Weeks 21–24)**Week 21 – Secure Development Lifecycle**

- ❖ Integration of cybersecurity in ASPICE & AUTOSAR
- ❖ CI/CD with security checks (static & dynamic analysis)
- ❖ Lab: Secure coding audit on ECU C code

Week 22 – Forensics & Incident Response

- ❖ Automotive logging strategies
- ❖ Post-attack analysis workflow
- ❖ Lab: Extract attack traces from CAN log files

Week 23 – Final Capstone Project (Build Secure ECU)

- ❖ Design & implement:
 - Secure Boot
 - HSM key storage
 - SecOC CAN communication
 - OTA with signature validation

Week 24 – Capstone Presentation & Industry Outlook

- ❖ Present project to peers (like an OEM security review)
- ❖ Latest industry trends: EV charging security, autonomous vehicle security, AI in IDS
- ❖ Career pathways for automotive cybersecurity

 Deliverables

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