# Syllabus: AUTOMOTIVE CYBERSECURITY FOR AUTOMOTIVE TECHNICIANS

## Part 1: Course Information

### Description:

***AUTOMOTIVE CYBERSECURITY FOR AUTOMOTIVE TECHNICIANS*** is an advanced automotive technology course that should be taken in the last semester of a two-year automotive technology associate degree program or towards the end of an advanced certificate program in the modern technology of automotive electronic systems. The goal of the course is to introduce students to the potential threats of cyber-attacks on vehicles, especially connected and automated vehicles.

The basics of cybersecurity threat models, high risk attack areas of vehicles, classes of attacks, and protecting vehicles from attacks are introduced. Standards and protocols related to automotive cybersecurity will be covered. Cybersecurity methods and penetration testing for vehicles will also be presented. Attacking connected vehicles will be discussed by reviewing vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications and wireless access protocols, such as IEEE 1609. Potential attacks on automated vehicles will be described. The course materials include a comprehensive course syllabus with the course outline and learning outcomes, a course roadmap showing where in the course the learning outcomes are covered, lecture handouts in Microsoft PowerPoint, homework assignments, quizzes, experiments, and course projects.

The course materials are suitable for community college students in automotive advanced certificate and/or associate degree programs students. The materials may also be adapted for use in the training of incumbent workers.

This course is designed to be a 3-credit course that will meet over a period of 15 to 16 weeks. In this format, it will consist of 2 meetings per week of 2 hours per meeting. Other formats are possible, such as a duration of 8 weeks with 8 hours of meeting time per week.

**Prerequisites** Basic electricity/electronics theory and/or automotive electronics basics

Basic knowledge of the operation of traditional vehicle systems: brakes, suspension and steering, drivetrain, engine, engine electrical, emission controls, fuel and exhaust systems, environmental systems, etc.

**Reference Books**
**The Car Hacker's Handbook, A Guide for the Penetration Tester, by Craig Smith (2016), ISBN-13: 978-1-59327-703-1**

## Part 2: Course Learning Outcomes (CLOs)

**The course learning outcomes are that the students:**

1. Understand potential cybersecurity threats for automotive systems;
2. Identify areas in cars with the highest risk components;
3. Understand threat modeling and identification in the automotive industry;
4. Understand the basics of threat rating systems for the cybersecurity of cars;
5. Become familiar with the various types of bus protocols and communications in vehicles;
6. Understand the concept of diagnostics/logging with security considerations;
7. Become familiar with important ISO and SAE standards from cybersecurity point of view and the roll of various organizations in the development and evolution of these standards;
8. Understand the basic concepts of automotive electronics and ECU from cybersecurity point of view;
9. Become familiar with ECU hacking and the roles of software and firmware in the hacking process;
10. Understand various methods of attacking vehicles;
11. Be familiar with classes of attack vectors in the current automotive industry;
12. Understand the fundamental principles of protocols and standards related to attacking vehicles;
13. Understand the In-vehicle infotainment (IVI) system
14. Become familiar with several remote attacking methods;
15. Become familiar with the concepts and standards for defining frameworks regarding cybersecurity of vehicles;
16. Understand the fundamentals of attacking connected/automated vehicles;
17. Become familiar with basics of V2V and V2I communication technology;
18. Become familiar with important standards and protocols regarding wireless access in vehicles;
19. Understand the potential for attacks on automated vehicles;
20. Become familiar with cybersecurity protection methods;
21. Understand penetration testing and related methods;

22. Demonstrate effective communication and teamwork skills through technical presentations and reports in course lab projects.

## Part 3: Course Topics and Roadmap

### Course Topics

1. Understanding Threat Models
    - Identify areas with the highest risk components
    - Threat modeling & identification
    - Threat rating systems
2. Bus Protocols & Vehicle Communication
    - CAN bus and diagnostic link connector (DLC) - OBD-II
    - CAN Bus Packet Layout
    - Media Oriented Systems Transport (MOST)
    - SocketCAN interface
    - Diagnostics/Logging, CAN Security, ISO-TP protocol
    - SAE J1698 Standard
3. Automotive Electronics and ECUs
    - Introduction to ECUs, software, and firmware
    - ECU Hacking
4. Attacking Vehicles
    - Classes of attack vectors
    - SAE J2534 & tools
    - In-vehicle infotainment (IVI) system & remote attacking
5. Defining Frameworks for Cybersecurity in Vehicles
    - J3061
    - ISO 21434
6. Attacking Connected/automated vehicles
    - V2Vand V2I communication
    - IEEE 1609 & Wireless Access in Vehicular Environments (WAVE)
    - Attacking Wireless Systems
    - Potential attacks on automated vehicles
7. Protecting Vehicles from Attacks
    - Cybersecurity protection methods
    - Penetration testing
    - Security Credentials Management System (SCMS)

**Course Roadmap**

The following roadmap is recommended for instructors (Handouts #1-7 are the PowerPoint lecture slides):

| Week and Topic | • Lecture Topics<br>• CLOs covered | Main Concepts, Terms, and Equations | • Course Materials,<br>• Homework & Projects |
|---|---|---|---|
| 1 | • Understanding Threat Models<br>• 1,2,3,4 | • Identify areas with the highest risk components<br>• Threat modeling & identification<br>• Threat rating systems | • Handout #1<br>• EX1<br>• Discussion of Lab and Course Projects |
| 2 | • Bus Protocols & Vehicle Communication<br>• 5 | • CAN bus and diagnostic link connector (DLC) - OBD-II<br>• CAN Bus Packet Layout | • Handout #2<br>• HW1 |
| 3 | • Bus Protocols & Vehicle Communication<br>• 5 | • Media Oriented Systems Transport (MOST)<br>• SocketCAN interface | • Handout #2<br>• Quiz1 |
| 4 | • Bus Protocols & Vehicle Communication<br>• 6,7 | • Diagnostics/Logging, CAN Security, ISO-TP protocol<br>• SAE J1698 Standard | • Handout #2<br>• HW2<br>• EX2 |
| 5 | • Automotive electronics and ECUs<br>• 8 | • Introduction to ECUs, software, and firmware | • Handout #3<br>• Quiz2<br>• Project 1 |
| 6 | • Automotive electronics and ECUs<br>• 8,9,22 | • ECU Hacking | • Handout #3<br>• EX3<br>• HW3 |
| 7 | • Attacking Vehicles<br>• 10,11 | • Classes of attack vectors | • Handout #4<br>• Quiz3 |

| | | | |
|---|---|---|---|
| 8 | • Attacking Vehicles<br>• 11 | • Classes of attack vectors | • Handout #4<br>• HW4 |
| 9 | • Attacking Vehicles<br>• 12,13,14 | • SAE J2534 & tools<br>• In-vehicle infotainment (IVI) system & remote attacking | • Handout #4<br>• Quiz4 |
| 10 | • Defining Frameworks for Cybersecurity in Vehicles<br>• 15,22 | • J3061<br>• ISO 21434 | • Handout #5<br>• EX4<br>• HW5 |
| 11 | • Attacking Connected/automated vehicles<br>• 16,17,18 | • V2Vand V2I communication<br>• IEEE 1609 & Wireless Access in Vehicular Environments (WAVE) | • Handout #6<br>• Quiz5 |
| 12 | • Attacking Connected/automated vehicles<br>• 19 | • Attacking Wireless Systems | • Handout #6<br>• HW6<br>• EX5 |
| 13 | • Attacking Connected/automated vehicles<br>• 19 | • Attacking Wireless Systems<br>• Potential attacks on automated vehicles | • Handout #6<br>• Project #2<br>• Quiz6 |
| 14 | • Protecting vehicles from attacks<br>• 20 | • Cybersecurity protection methods<br>• Penetration testing | • Handout #7<br>• HW7 |
| 15 | • Protecting vehicles from attacks<br>• 21,22 | • Penetration testing<br>• Security Credentials Management System (SCMS) | • Handout #7<br>• Quiz7 |
| | | | |

## Part 4: Grading and Assessment

### HW Assignments

The seven homework (HW) assignments are related to the topics described above. They will be collected and graded and are part of the overall course grade. They will be available as a separate document.

### Quizzes

A quiz will be given on each of the seven topics.

### Course Projects

Two course projects are to be assigned. The first one is about emulating a CAN signal. The second project is about RF key fob hacking. The second project is divided into two parts and can be done as a group project.

### Course Experiments Work and Lab Projects

The student will be assigned laboratory experiments (EX) to complete. These experiments might include Internet research about the course topics, hands-on activities with sensors and microcontrollers, emulating CAN bus, and wireless transceivers and hacking. A list of possible lab exercises and laboratory projects is included as a separate document.

### Computer Usage

Students should be able to use a PC, be familiar with a recent Windows OS, and be comfortable accessing information from the Internet

### Tools to be used

For the course, students should possess basic PC skills and have a knowledge of Microsoft Office (specifically, Microsoft Word and Power Point). For the lab portion of the course, please refer to the documents that speak to those activities.

### Grading Schedule

| | |
|---|---|
| ➢ Homework | 14% |
| ➢ Quizzes | 28% |
| ➢ Course Projects | 30% |
| ➢ Experiments | 28% |

**Prepared by:** Professor Mehrdad Zadeh, Ph.D., Kettering University
**Email** mzadeh@kettering.edu
**Work Phone** 810-762-9500, Ext. 5914
**Office Location** AB 2-703P

**Date**: 3/20/2019
**Revised:** 8/1/2019