MAGMA

Michigan Alliance for Greater Mobility Advancement

Course Title: Automotive Cybersecurity: Attacking & Protecting Connected/Automated Vehicles

Course Length: 2 days

Time Online: 2 hours

Time in Class: 6 hours (Lab and Class) per day

Time in Lab: 4 hours (2 hours per day)

Class Size: Minimum 7 / Maximum 12

Price Per Student: $2,310.00*

Location: Company Site

Course Description:

Cybersecurity has a wide range of definitions in different areas such as Internet, Automotive, IoT, Network, Smart Device, to name a few. More generally, it comprises modules, which protect computer-based systems from being attacked, hacked, or manipulated, intentionally. In addition, protection is applied in whether software or hardware part of systems. Advent of IoT and its applications in vehicles, cybersecurity involved to automotive industry in order to establish safety. Furthermore, the paramount goal of automotive industry is to develop fully autonomous vehicles. This will be achieved by employing sophisticated hardware and software components, which are potentially susceptible to threats with different purposes. To this end, it is requisite for those who work in this industry to have a profound knowledge of how threats influence on vehicle's components and connectivity as well as methods to handle harmful situations.

This course is an advanced hands-on automotive technology course that focus on cybersecurity challenges for connected/automated vehicles. In addition, an overview will be presented on topics such as threats models, high risk areas of cars, classes of attacks, automotive electronics (hardware & software), and protecting vehicles from attacks. and covers their functionality in both software and hardware parts. This course covers protocols in the communication part of vehicles in order to explain means of penetration. A description of threat models is provided for the purpose of acquainting student with the behavior of threats in every component. This helps students to discriminant between inadvertent and intentional defects through the vehicle's electronical components. In addition, students get familiar with various methods and tools for attacking vehicles component such as remote attacking. Using these concepts, students then learn about cybersecurity methods and penetration testing for connected/automated vehicles. Attacking connected vehicles will be discussed in detail by reviewing vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications and wireless access protocols, such as IEEE 1609.

* Price based on minimum enrollment, subject to change

Potential attacks on automated vehicles will be described as well. In particular, the intended course comprises:

- Online material
- Two-day in-class interactive presentation.
- Lab projects

Students should take the online material prior to the in-class presentation to acquire an outline of the course contents. Subsequently, students will attend face-to-face interactive classes after they successfully pass the online course. The presentation has been divided into several parts based on the syllabus so that every part covers one topic of the syllabus. The instructor takes a quiz after each part to evaluate the retention of course materials. Several lab projects have been designed using low-cost hardware platforms that will be completed in two days of course.

Lab Projects Description:

The main goal of lab projects is to provide students opportunities for acquiring hands-on skills and demonstrate the practical applications of the course topics. Proposed projects are listed as follows:

Project 1: Building and using ECU test benches

Lab Main Purpose:

The following experiment has been designed to familiarize the trainees with attacks techniques in the embedded systems to address security problem in the automotive. This has been made up of creating setup procedures as well as applying attacks methods by using aforementioned setup.

Lab Description

The experiments aid students to identify chips and monitor power usage to create a profile of good operations. They would be able to test whether password checks could be attacked by monitoring the power output of bad characters in passwords, ultimately to create a brute-forcing application using power analysis to cut the password brute-force time down to seconds. Also they can see how clock and power glitching can make instructions skip at key points in the firmware's execution, such as during validation security checks or when setting JTAG security.

Lab outline:

Side-Channel Analysis with the ChipWhisperer

- Installing the Software
- Prepping the Victim Board
- Brute-Forcing Secure Boot Loaders in Power-Analysis Attacks

- Prepping Your Test with AVRDUDESS
- Setting Up the ChipWhisperer for Serial Communications
- Setting a Custom Password
- Resetting the AVR
- Setting Up the ChipWhisperer ADC
- Monitoring Power Usage on Password Entry

Project 2: Decoding RF Signals (RF Key fob Hacking)

In this lab, students will be decoding the signals emitted from the key fob. Flash the "Receiver_Part1" onto the receiver Arduino board.

1. Open the Serial Monitor in the Arduino IDE (Tools > Serial Monitor).
2. Press one of the buttons of the key fob.
3. The data read from the RF receiver will print out in the Serial Monitor window.
4. Copy the data from the Serial Monitor and paste it into Excel or Google Sheets.
    a. If you cannot paste directly then paste the data into a text file first.
    b. Delete the header on the data (Highlighted below) and save the file as a "CSV".
    c. You can now import the CSV file into Excel or Google Sheets.
5. Using either Excel or Google Sheets trim your data down to the transmission section. Refer to the blog post to see what this should look like.

Project 3: Hack the fob!

In this section you will be using both Arduino boards to hack the key fob. Instead of analyzing the raw frequency changes of the RF we will be using an encoder/decoder called RCSwitch.

Adding Libraries to Arduino IDE

1. In a sketch click on "Tools" then select "Manage Libraries"
2. In the filter type "RCSwitch".
3. Click Install.
4. Restart Arduino IDE.

Procedure:

1. Flash the "RC_RX_1" code file onto the receiver board.
    a. Unplug the receiver board from your computer and connect to the wall for power using the wall power supply. This is not necessary but it does help remove any confusion when flashing the hacker board.
2. Test the key fob to see if it correctly turns the LED on the receiver board on/off.
3. Complete the missing code in the "RC_TX_1" and compile it until there are no errors.
4. Flash the "RC_TX_1" code file onto the hacker board.

5. With both of the boards powered, open the Serial Monitor for the hacker board and put it into recording mode (Button 1 next to the RF transmitter).
6. Press the desired button on the key fob.
7. The signal should be recorded. Now you should be able to control the LED with the transmit button on the hacker board.
8. Redo the recording by resetting the hacker board and trying different buttons on the key fob.

<u>Course Learning Objectives:</u>

Over the recent years, emerging computer-based components in the structure of vehicles, attracting more attentions toward the role of computer engineering facets. This has led software as well as hardware to be responsible of functionality, in cooperation with mechanical parts within vehicles. Although, it has facilitated programmability and connectivity between vehicles, the possibility of an eclectic range of threats such as hacking and attacking has raised, accordingly. It has become more accentuated by the advent of autonomous vehicles. With this in mind, having a comprehensive knowledge of threats and its corresponding goals and purposes, seems to be crucial for professionals in this industry. For this reason, firstly, this course aims to make students familiar with those electronic parts of vehicles, which are potentially exposed to be hacked or attacked. Using aforementioned knowledge, they can effectively understand different ways of penetrations. Secondly, common methods of threats are discussed in detail in such a way that students not only learn how threats occur but also, they are trained to carry out a sample of hacking on their own. This helps them to confront a real hacking or attacking situation and acquire hands-on skills to learn about potential threats and protecting vehicles from attacks. Eventually, they need to protect products in automotive industry from being vulnerable to the threats and make them secure against harmful attacks, unauthorized access, damage, or any interferences with safety functions. Therefore, they obtain essential information on protection methods in order to elevate their proficiency and create new design or modify former one based on cyber security concepts. Each student who receives credit for this course will have demonstrated the ability to:

- Explain potential cybersecurity threats for connected/automated vehicles
- Identify areas in connected/automated vehicles with the highest risk components
- Configure and develop experimental test plans for modeling attacks on connected/automated vehicles
- Perform experiments using low-cost platforms according to test plans
- Explain important ISO and SAE standards from cybersecurity point of view and the roll of various organizations in the development and evolution of these standards
- Differentiate various methods of attacking connected/automated vehicles
- Articulate the In-vehicle infotainment (IVI) system remote attacking methods
- Explain important standards and protocols regarding wireless access in vehicles
- Demonstrate familiarity with cybersecurity protection methods

- Explain penetration testing and related methods
- Demonstrate effective communication and teamwork skills through technical presentations and reports in course lab projects

Course Content/Syllabus:

This course has an online material, interactive class presentation, which is followed by a lab project. Students should pass the online course prior to the presentation. This provides them a baseline of topics, which are going to be discussed in the class. In-class presentation will be taught in two successive days. A lab project will be completed by the end of each day.

Online course:

Students should take this course one week prior to attending in-class presentation. They will obtain an outline of all contents, which are going to be discussed in the class. They will learn following topic:

- Understanding Threat Models
- Bus Protocols & Vehicle Communication
- Automotive electronics and ECUs
- Attacking vehicles
- Defining Frameworks for Cybersecurity in Vehicles

Student will take a quiz on the covered topics and send their answers to the instructor via email.

Day 1:

The online course will be followed by a successive two-day in-class presentation. In the first day, the instructor will enlighten those who have questions from contents of the online course. After that, students will obtain more information about highest risk areas/components in connected/automated vehicles, threat models, protocols in detail. Having knowledge vehicles electronics/sensors, students will be able to do the first lab project. The topics of this class are listed as follows:

Topics:

- History & cybersecurity awareness
- Overview of V2Vand V2I communication
- Highest risk areas/components in connected/automated vehicles
- Overview of CAN bus and diagnostic link connector (DLC) - OBD-II

- Threat modeling, identification, and rating systems for connected/automated vehicles
- Diagnostics/Logging, CAN Security, ISO-TP protocol
- Overview of ECU hacking: software and firmware

Day 2:

In the next day, the class will be in an interactive way and the instructor will review contents of previous sessions and engross students in challenging issues of threat modeling. In this day, student will become familiar with attack methods, communication between vehicles and corresponding attack models on connected/automated cars, wireless attacks and protection methods. At end of this class, they will complete one lab project or two projects if time permits.

Topics:

- Potential attacks on connected/automated vehicles
- Attacks using various sensors in connected/automated vehicles (GPS, LiDAR, IMU, Camera)
- Adversarial attacks & Deep Neural Network (DNN)
- Classes of attack vectors
- In-vehicle infotainment (IVI) system & remote attacking
- IEEE 1609 & Wireless Access in Vehicular Environments (WAVE)
- Attacking Wireless Systems
- Cybersecurity protection methods for connected/automated vehicles
- Penetration testing