**Course Experiments**

**Automotive Cybersecurity for Automotive Technicians**

The following lab experiments are potential assignments to practice hands-on skills related to the course materials.

**Experiment 1: Getting Familiar with Course Tools for Packet Sniffing.**

Tutorial on Wireshark, Nmap, and Fiddler

**Lab Main Purpose:**

Understand some tools for hacking and beginning to understand how to learn multiple tools for many things

**Lab Description:**

In this course, you will use some following tools for hacking from a variety:

* Wireshark
  + <https://www.youtube.com/watch?v=TkCSr30UojM>
* Nmap
  + <https://www.youtube.com/watch?v=3Ab1gw8vQjg>
  + <https://www.youtube.com/watch?v=TJwz1Xyxmc8>
* Fiddler
  + <https://www.youtube.com/watch?time_continue=327&v=LWPeVPRjl0o>

These tools will enable the user to sniff packets of Wi-Fi data and allow user to start deciphering and receiving unwanted data. All three are download loadable to windows platform and with something as cheap as a wireless adapter can be used quietly to record data. TP-Link 150Mbps High Gain Wireless USB Adapter is one of these adapters for roughly $10 that can start this sniffing off.

**Lab outline:**

Download and complete these tutorials on each software to gain a basic understanding of software tool sets

**List of required materials:**

Windows computer or Linux computer. NOTE: Preferably a Linux computer.

**Experiment 2:**

Pi to Pi with CAN

**Lab Main Purpose:**

Hack CAN communication between the Pis.

**Lab Description:**

Students will record and analyze the CAN signals being sent between the Raspberry pis.

**Lab outline:**

Have two Raspberry Pis with appropriate CAN interface shields communicate to each other. One raspberry pi will have a LED light attached to it. The communication line between the Pis will be split with another wire and an OBD-II port. The LED on the raspberry pi will be controlled by the opposite pi by a toggle single sent every second or so over CAN. Good resources for more information:

[https://www.elektor.com/pican-2-can-bus-board-for-raspberry-pi#description](https://www.elektor.com/pican-2-can-bus-board-for-raspberry-pi" \l "description)

**List of required materials:**

Alongside wiring and some other miscellaneous parts such as an LED the items below are the recommended parts for this lab:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Part Name** | **Link** | **Quantity** | **Piece Cost** | **Total Cost** |
| PiCAN 2 (Can Find Cheaper) | [HERE](https://copperhilltech.com/pican-2-can-interface-for-raspberry-pi-2-3/) | 2 | 49.95 | 99.90 |
| Raspberry Pi 3 | [HERE](https://www.adafruit.com/product/3055?src=raspberrypi) | 2 | 35.00 | 70.00 |
| OBD-II Connector | [HERE](https://www.kr4.us/obd-ii-connector.html?gclid=Cj0KCQjwnpXmBRDUARIsAEo71tQGi4DffZ8et7Qm3JsgJfCSWC7-YiCcScwR3cuv_WUDd1QpIslSKRkaAsGnEALw_wcB) | 1 | 3.95 | 3.95 |
| OBD-II to USB cable | [HERE](https://www.walmart.com/ip/OBD2-OBDII-KKL-VAG-COM-409-1-USB-Interface-Diagnostic-Cable-For-AUDI-Volkswagen/894906604?wmlspartner=wlpa&selectedSellerId=18038&adid=22222222227239619664&wl0=&wl1=g&wl2=c&wl3=286016965904&wl4=aud-566049426705:pla-507938826634&wl5=9017029&wl6=&wl7=&wl8=&wl9=pla&wl10=125210912&wl11=online&wl12=894906604&wl13=&veh=sem&gclid=Cj0KCQjwnpXmBRDUARIsAEo71tRfNgk9g56CL-anOra9Y8_XEG-YiceoR0SfgozC3cnQvkGi5xGDufgaAitrEALw_wcB) | 1 | 8.50 | 8.50 |
|  |  |  | **Total Cost** | **182.35** |

NOTE: All parts listed are the recommended parts, not the required models. I can imagine that there are cheaper options for nearly all of the parts listed especially the PiCAN 2 shield.

**Experiment 3:**

**Building and using ECU test benches**

**Lab Main Purpose:**

In the following experiment, student will learn how build an ECU test bench in an affordable manner for having a safe vehicle security testing.

**Lab Description**

The experiments use ECU or simulator as a required tool. Students can get familiar to the different parts of ECU and learn how to read wiring diagram. Also, they will learn how to build a more advanced test bench that can simulate engine signals in order to trick components into thinking the vehicle is present. To achieve the targets, chapter 7 of “THE CAR HACKER’S HANDBOOK A Guide for the Penetration Tester” is a good source to follow.

**Lab outline:**

Following items will be done:

* Getting familiar with ECU
* Communicating with ECU via wire.
* Simulating sensor data: Coolant temperature sensor, Fuel sensor, Oxygen sensors, Throttle position, Pressure sensors and Vehicle Speed.

**List of required materials:**

Personal car’s ECU or ordering online on <http://car-part.com/>

or

Using prebuilt simulator ECUsim 2000 by ScanTool.

It is notable that a simulator like ECUsim will cost around $200 per protocol and will support only OBD/UDS communications.

**Experiment 4:**

**ECU Attacking**

**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:**

Since the reference of the following experiment is topic “Attacking Vehicle” and chapter 8 of “THE CAR HACKER’S HANDBOOK A Guide for the Penetration Tester” indirectly, approaching to below items is considered. It is worth to say that the experiment titles come from the sub topic of course reference:

* 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

**List of required materials:**

* Basic knowledge of computer programming with Python.
* A good understanding of basic electronics.

**Experiment 5:**

RF Sniffing and Transmitting

**Lab Main Purpose:**

Record RF signals and replay them back to control some RF based device.

**Lab Description:**

Students will learn how to control a basic radio frequency controlled device by recording the signals emitted from a key fob and play them back to turn on a LED connected to an Arduino/Raspberry Pi.

This is a very well written series of tutorials on RF transmission and reception. The lab would be written to follow this with some basic changes. From a automotive cyber security perspective, this could be extrapolated to hacking or gaining entrance to a vehicle from the wireless key fob.

<https://arduinobasics.blogspot.com/2014/06/433-mhz-rf-module-with-arduino-tutorial.html>

**List of required materials:**

Parts listed below are the core components for this project. Aside from what is listed some basic components are needed such as 330 Ohm resistors, LEDs, and wires. These pieces are not included in the cost due to their trivial cost and general abundance.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Part Name** | **Link** | **Quantity** | **Piece Cost** | **Total Cost** |
| Remote Wireless Keyfob 315MHz | [HERE](https://www.dfrobot.com/product-1090.html) | 1 | $5.20 | $5.20 |
| RF wireless receiver and transmitter module | [HERE](https://www.newegg.com/Product/Product.aspx?Item=9SIADG45WH8060&ignorebbr=1&source=region&nm_mc=KNC-GoogleMKP-PC&cm_mmc=KNC-GoogleMKP-PC-_-pla-Keyboardmall-_-Gadgets-_-9SIADG45WH8060&gclid=Cj0KCQjwh6XmBRDRARIsAKNInDFtUtdv3bpHlVC7zrarHA8jnYT2uAt1UgIRV0eMVR1YcYx8J5KsozkaAif-EALw_wcB&gclsrc=aw.ds) | 2 | $7.99 | $15.98 |
| Arduino UNO | [HERE](https://www.amazon.com/Development-Microcontroller-ATmega328-ATMEGA16U2-Original/dp/B07MMMSNYH/ref=sr_1_1_sspa?gclid=Cj0KCQjwh6XmBRDRARIsAKNInDGn25CQNS-yJXAS4ctdwGU_0-WEpqj2YWc7MUyKh8byyDooTTUqlwQaArfzEALw_wcB&hvadid=269674964635&hvdev=c&hvlocphy=9017029&hvnetw=g&hvpos=1t1&hvqmt=e&hvrand=16142071861063206483&hvtargid=kwd-31430758221&hydadcr=19104_10726406&keywords=arduino+uno+r3&qid=1556744692&s=gateway&sr=8-1-spons&psc=1) | 2 | $16.99 | $33.98 |
|  |  |  | **Total Cost** | $55.16 |

NOTE: All parts listed are the recommended parts, not the required models. I can imagine that there are cheaper options for nearly all of the parts listed.