## List of equipment used in testing.

The tools needed to conduct the experiments are On-Board Diagnostic (ODB) reader/scanner tools. They are a 16-pin tools that plug into the data port. These tools are OBDII scanners and the “II” is at is a designation of second generation of the port. Once they are plugged in, they can open up your vehicle computer to the world (if network enabled). Also needed was Android software to connect to the Bluetooth scanner. The app is Torque Pro version 1.10.120 by Ian Hawkins. This app runs on an Android phone.

## Tests conducted with Autophix OM126 OBDII.

The Autophix OM126 is not network capable. The tests were run on a 2002 Ford Taurus v6 engine. I disconnect several hoses in the engine. The scan tool then found several codes: P0300 – Random/Multiple Cylinder Misfire Detected, P1151 and P1131 – Lack of HO2S21 Switches – Sensor Indictes Lean, P0442 – EVAP System Leak Detected (small leak). I was able to fix the hoses and cleared the codes with the tool.

The attack vectors with this tool are stealing data and altering data. The codes can be cleared even if the problems were not fixed. This violates Confidentiality, Integrity and Availability (CIA). Also, some basic information like the Vehicle Identification Number (VIN), Calibration Identifications (CID) and Calibration Verification Numbers (CVN) could be stolen and used for malicious purposes. The attack vectors are minimal for this device since there is no network connectivity.

## Tests conducted with Veepeak OBDCheck BLE+ Bluetooth 4.0

The Next test was with the Veepeak OBDCheck BLE+ Bluetooth 4.0. This tool is Bluetooth capable. The vehicle tested was a 2008 VW Jetta with a 2.5 Liter engine. The test included using two vehicles, first vehicle with the OBD scanner connected to the 16-pin data port and the 2nd vehicle I rode in using my Android phone running the Torque Pro app. While both vehicles were driving, I pulled up close to the back of the first vehicle and scanned for Bluetooth devices. Several signals were found but I found the Veepeak device and connected. I tested different distances and found that 20 feet was about max where I could connect. I then recorded data from the vehicle for GPS location, latitude, longitude, Altitude, etc. With the app I saved the data into a file and emailed it to my address.

The attack vectors were expanded with this test due to network capability. There was also a web interface you can send data to. This also violated CIA.

## Autel scanner MK808 research

The other tool that I researched but did not purchase was the Autel scanner MK808 and has 25 service functions [25]. The capability is well beyond the basic vehicle diagnostic code scanner. It supports vehicle ECUs ISO9141-2, ISO14230-2,ISO15765, K/L-Line, Flashing Code, SAE-J1850 VPW, SAE-J1850 PWM, ISO11898(Highspeed, Middlespeed, Lowspeed and Singlewire CAN,fault-tolerant CAN), SAE J2610,GM UART,UART Echo Byte Protocol, Honda Diag-H Protocol, TP2.0 and TP1.6 [26]. Most cars today including Electric Vehicles are represented in this list.

The following functions can be done:

* Oil Reset, to reset the oil service lamp for the engine oil life system.
* EPB Reset, to reset the brake pad after replacing the brake pad.
* Injector Coding, to write the new code to the ECU after replacement of injector.
* ABS Bleeding, to perform various bi-directional tests of Anti-lock Braking System.
* DPF Reset, to retrieve/erase DPF-related codes, and reset the DPF light.
* IMMO Service, to disable the lost key and add the new key’s data for security in Asian cars.
* BMS Reset, Throttle Matching, TPMS Reset, SAS Calibration, Suspension Calibration, Trans Adaption, Airbag Reset, ABS & SRS, WIN DR Roof, Seats, Lang Change, Headlamp, CHG Tire Size, TEC Learn, Cylinder, Odometer, Turbocharging, Clutch, A/F Setting.

This tool supports Wi-fi and is very cable of doing advanced exploits on a vehicle. Some of the exploits would be to disable the keys and add new key’s data. An attacker could drive alongside your vehicle, do the exploits and then follow you to steal your car. Another example is to set the ignition timing so far advanced that it causes detonation, which can destroy the engine.

These tests were all done without authentication from the driver.