



Features Business Explore Marketplace Pricing

This repository

Search

Sign in or Sign up

jaredthecoder / awesome-vehicle-security

Watch

72

★ Star

748

🍴 Fork

211

<> Code

! Issues 0

🔗 Pull requests 0

📊 Insights

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

🚗 A curated list of resources for learning about vehicle security and car hacking.

vehicle-security

car-hacking

hacking-vehicles

security

hardware

learning

hacktoberfest

📦 157 commits

🌿 1 branch

📦 0 releases

👥 29 contributors

📄 CC0-1.0

Branch: master ▾

New pull request

Find file

Clone or download ▾







jaredthecoder Merge pull request #40 from trollwookiee/pandwarf-hw-add ...

Latest commit efd171a on Apr 7

📁 assets

Add two gifs and update README.md

2 years ago

 LICENSE	Initial commit	2 years ago
 README.md	Add PandwaRF hardware	3 months ago
 _config.yml	Set theme jekyll-theme-cayman	7 months ago
 contributing.md	Update contributing.md	7 months ago

README.md

Awesome Vehicle Security

A curated list of awesome resources, books, hardware, software, applications, people to follow, and more cool stuff about vehicle security, car hacking, and tinkering with the functionality of your car.



I would love as much help as I can get. [Start contributing!](#)

Follow me on [Twitter](#) for more security goodness.

Contents

- [Learn](#)
 - [Articles](#)
 - [Presentations](#)

- [Books](#)
- [Research Papers](#)
- [Courses](#)
- [Blogs](#)
- [Websites](#)
- [Newsletters](#)
- [Conferences](#)
- [Who to Follow](#)
- [Podcasts and Episodes](#)
 - [Podcasts](#)
 - [Episodes](#)
- [Projects](#)
- [Hardware](#)
- [Software](#)
 - [Applications](#)
 - [Libraries and Tools](#)
 - [C](#)
 - [Python](#)
 - [Go](#)
 - [JavaScript](#)
- [Companies and Jobs](#)
 - [Coordinated Disclosure](#)
- [Other Awesome Lists](#)
- [Contributing](#)

Learn

Articles

- [How to hack a car—a quick crash-course](#) - Car enthusiast Kenny Kuchera illustrates just enough information to get you up and running. An excellent resource for first timers!
- [Stopping a Jeep Cherokee on the Highway Remotely](#) - Chris Valasek's and Charlie Miller's pivotal research on hacking into Jeep's presented at DEFCON in 2015.
- [Troy Hunt on Controlling Nissans](#) - Troy Hunt goes into controlling Nissan vehicles.
- [Tesla hackers explain how they did it at Defcon](#) - Overview of DEFCON 23 presentation on hacking into Tesla cars.
- [Anatomy of the RollJam Wireless Car Hack](#) - Overview of the RollJam rolling code exploitation device.
- [IOActive's Tools and Data](#) - Chris Valasek and Charlie Miller release some of their tools and data for hacking into vehicles in an effort to get more people into vehicle security research.
- [Developments in Car Hacking](#) - via the SANS Reading Room, Currie's paper analyses the risks and perils of smart vehicle technology.
- [Car Hacking on the Cheap](#) - A whitepaper from Chris Valesek and IOActive on hacking your car when you don't have a lot of resources at your disposal.
- [Car Hacking: The definitive source](#) - Charlie Miller and Chris Valasek publish all tools, data, research notes, and papers for everyone for free
- [Car Hacking on the cheap](#) - Craig Smith wrote a brief article on working with Metasploit's HWBrige using ELM327 Bluetooth dongle
- [Researchers tackle autonomous vehicle security](#) - Texas A&M researchers develop intelligence system prototype.
- [How big data will impact car security in the proximate future: Concerns and solutions](#) - Impact of big data on car security.

Presentations

- ["Hopping on the CAN Bus" from BlackHat Asia 2015](#) - A talk from BlackHat Asia 2015 that aims to enable the audience to "gain an understanding of automotive systems, but will also have the tools to attack them".
- ["Drive It Like You Hacked It" from DEFCON 23](#) - A talk and slides from Samy Kamkar's DEFCON 23/2015 talk that includes hacking garages, exploiting automotive mobile apps, and breaking rolling codes to unlock any vehicle with low cost tools.
- [Samy Kamkar on Hacking Vehicles with OnStar](#) - Samy Kamkar, the prolific hacker behind the Samy worm on MySpace, explores hacking into vehicles with OnStar systems.
- [Remote Exploitation of an Unaltered Passenger Vehicle](#) - DEFCON 23 talk Chris Valasek and Charlie Miller give their now famous talk on hacking into a Jeep remotely and stopping it dead in its tracks.
- [Adventures in Automotive Networks and Control Units](#) - DEFCON 21 talk by Chris Valasek and Charlie Miller on automotive networks.
- [Can You Trust Autonomous Vehicles?](#) - DEFCON 24 talk by Jianhao Liu, Chen Yan, Wenyuan Xu
- [Ken Munro & Dave Lodge - Hacking the Mitsubishi Outlander & IOT](#) - talk from BSides Manchester 2016 by Ken and Dave of [Pen Test Partners](#)
- [A Platform base on Visualization for Protecting CAN Bus Security](#) - Syscan360 2016 SH talk by Jianhao Liu
- [Gateway Internals of Tesla Motors](#) - Zeronights 2016 talk by Nie Seng and Liu Ling
- [Car Hacking 101](#) - Bugcrowd LevelUp 2017 by Alan Mond
- [State of Automotive Cyber Safety, 2015](#) - State of automotive hacking, policy, industry changes, etc. from I Am The Cavalry track at BSides Las Vegas, 2015.
- [State of Automotive Cyber Safety, 2016](#) - State of automotive hacking, policy, industry changes, etc. from I Am The Cavalry track at BSides Las Vegas, 2016.
- [How to Hack a Tesla Model S](#) - DEF CON 23 talk by Marc Rogers and Kevin Mahaffey on hacking a Tesla. Tesla Co-Founder and CTO, JB Straubel, joins them to thank them and present a challenge coin.

- [Car Hacking Videos](#) - A web page with a long list of videos (40+) that are available online related to the topic of car hacking. From a 2007 DEF CON talk on modding engine ECUS and onwards (e.g. the 2017 Keen Security Tesla hack).
- [Self-Driving and Connected Cars: Fooling Sensors and Tracking Drivers](#) - Black Hat talk by Jonathan Petit. Automated and connected vehicles are the next evolution in transportation and will improve safety, traffic efficiency and driving experience. This talk will be divided in two parts: 1) security of autonomous automated vehicles and 2) privacy of connected vehicles. 2015
- [A Survey of Remote Automotive Attack Surfaces](#) - Black Hat talk By Charlie Miller and Chris Valasek. Automotive security concerns have gone from the fringe to the mainstream with security researchers showing the susceptibility of the modern vehicle to local and remote attacks. Discussion of vehicle attack surfaces. 2014.
- [Pentesting vehicles with YACHT \(Yet Another Car Hacking Tool\)](#) -A presentation that discusses different attack surfaces of a vehicle, then continues to describe an approach to car hacking along with tools needed to analyse and gather useful information.

Books

- [2014 Car Hacker's Handbook](#) - Free guide to hacking vehicles from 2014. You can also buy the book on Amazon [here](#).
- [2016 Car Hacker's Handbook](#) - Latest version of the Car Hacker's handbook with updated information to hack your own vehicle and learning vehicle security. For a physical copy as well unlimited PDF, MOBI, and EPUB copies of the book, buy it at [No Starch Press](#). Sections are available online [here](#).
- [A Comprehensive Guide to Controller Area Network](#) - An older book from 2005, but still a comprehensive guide on CAN buses and networking in vehicles.
- [Controller Area Network Prototyping with Arduino](#) - This book guides you through prototyping CAN applications on Arduinos, which can help when working with CAN on your own car.
- [Embedded Networking with CAN and CANopen](#) - From 2003, this book fills in gaps in CAN literature and will educate you further on CAN networks and working with embedded systems.

Research Papers

- [Koscher et al. Experimental Security Analysis of a Modern Automobile, 2010](#)
- [Comprehensive Experimental Analyses of Automotive Attack Surfaces, 2011](#)
- [Miller and Vasek - Self proclaimed "car hacking the definitive source".](#)
 - [Adventures in Automotive Networks and Control Units \(aka car hacking\)](#)
 - [Car Hacking for Poories](#)
 - [A Survey of Remote Automotive Attack Surfaces, 2014](#)
 - [Remote Compromise of an Unaltered Passenger Vehicle \(aka The Jeep Hack\), 2015](#)
 - [Advanced CAN Message Injection, 2016](#)
- [5-Star Automotive Cyber Safety Framework, 2015](#)
- [A Vulnerability in Modern Automotive Standards and How We Exploited It](#)
- [A Car Hacking Experiment: When Connectivity Meets Vulnerability](#)
- [Security issues and vulnerabilities in connected car systems](#)
- [Automobile Driver Fingerprinting, 2016](#)

Courses

- [Udacity's Self Driving Car Engineer Course](#) - The content for Udacity's self driving car software engineer course. The actual course on Udacity's website is [here](#).

Blogs

- [Keen Security Lab Blog](#) - Blog created by Keen Security Lab of Tencent that posts research on car security.

Websites

- [OpenGarages](#) - Provides public access, documentation and tools necessary to understand today's modern vehicle systems.
- [DEFCON Car Hacking Village](#) - Car Hacking exercises from DEFCON 24.
- [canbushack: Hack Your Car](#) - course on Vehicle Hacking methodology.
- [OWASP Internet of Things Project](#) - OWASP's project to secure IoT, from cars to medical devices and beyond.
- [I Am The Cavalry](#) - Global grassroots (eg. volunteer) initiative focused on the intersection of security and human life/public safety issues, such as cars. Participation from security researchers, OEMs, Tier 1s, and many others. Published [Automotive 5-Star Cyber Safety Framework](#).
- [Carloop Community](#) - Community of people interested in car hacking and connecting vehicles to the cloud.
- [Python Security](#) - A website for browsing and buying python-integrated cars having certain vehicular security features.

Newsletters

[Welcoming contributions!](#)

Conferences

- [U.S. Automotive Cyber Security Summit European Automotive Cyber Security Summit](#) - Conference series dedicated to automotive cyber security involving many OEMs, Tier 1s, academics, consultants, etc.
- [escar conference](#) - Embedded security in cars. European event has run for over 10 years, and they now have US and Asia events.
- [IT Security for Vehicles](#) - Conference run by the Association of German Engineers (VDI), with participation from US and European OEMs, Tier 1s, and others.

Who to Follow

- Chris Valasek: Security Lead at [UberATC](#)
 - [Twitter](#)
 - [Website](#)
- Charlie Miller: Hacked the first Apple iPhone, now does car security.
 - [Twitter](#)
- Samy Kamkar: Created MySpace Worm, RollJam, OwnStar.
 - [Twitter](#)
 - [Website](#)
- Justin Seitz: Author of Black Hat Python (No Starch Press).
 - [Twitter](#)
- Troy Hunt: Pluralsight author. Microsoft Regional Director and MVP for Developer Security. Creator of [haveibeenpwned](#).
 - [Twitter](#)
 - [Website](#)
- Ken Munro: British researcher, works at Pen Test Partners; major interest in vehicle security
 - [Twitter](#)
- OpenGarages: Initiative to create Vehicle Research Labs around the world.
 - [Twitter](#)
 - [Website](#)
- Hackaday: Collaborative project hosting for hackers - there are frequently car projects on here.
 - [Twitter](#)
- Pen Test Partners: British penetration testing firm; several posts concern their disclosed car security vulns
 - [Twitter](#)
 - [Website](#)

- I Am The Cavalry: Global grassroots (eg. volunteer) initiative focused on the intersection of security and human life/public safety issues, such as cars.
 - [Twitter](#)
 - [Website](#)
 - [Discussion Group](#)

Podcasts and Episodes

Podcasts and podcast episodes, that either directly focus on vehicle security or have some episodes on it.

Podcasts

- [Security Weekly](#) - Excellent podcast covering all ranges of security, with some episodes focusing portions on vehicle security from cars to drones.
- [TrustedSec Podcast](#) - From the people at TrustedSec, leaders in Social Engineering, their episodes often go into recent vehicle vulnerabilities and exploits.
- [SANS Internet Storm Center](#) - the ISC run a regular podcast going into the latest vulnerabilities and security news.
- [Security Ledger](#) - A podcast focusing on interviewing security experts about topics related to security.

Episodes

- [Car Hacking with Craig Smith](#) - Software Engineering Daily did an amazing episode with Craig Smith, author of the Car Hacking Handbook (above), on hacking into vehicles.
- [Big Bugs Podcast Episode 1: Auto Bugs - Critical Vulns found in Cars with Jason Haddix](#) - Jason Haddix explores major vulnerabilities found in cars.
- [Hacking Under the Hood and Into Your Car](#) - Chris Valasek and Charlie Miller discuss with NPR how they were able to hack into vehicles.

- [Hacking Connected Vehicles with Chris Valasek of IOActive](#) - Chris Valasek talks about hacking into connected vehicles.
- [Hackable? - Cars are Computers](#) - Geoff Siskind paired up with Craig Smith, author of The Car Hacker's Handbook, to show us just how easy – or not – it is to hack a car.

Projects

- [Open Vehicle Monitoring System](#) - A community project building a hardware module for your car, a server to talk to it, and a mobile app to talk to the server, in order to allow developers and enthusiasts to add more functionality to their car and control it remotely.
- [Open Source Car Control Project](#) - The Open Source Car Control Project is a hardware and software project detailing the conversion of a late model vehicle into an autonomous driving research and development vehicle.

Hardware

Overview of hardware, both open source and proprietary, that you can use when conducting vehicle security research. [This article](#) goes through many of the options below.

- [Arduino](#) - Arduino boards have a number of shields you can attach to connect to CAN-enabled devices.
 - [CANdiy-Shield](#)
 - [ChuangZhou CAN-Bus Shield](#)
 - [DFRobot CAN-BUS Shield For Arduino](#)
 - [SparkFun CAN-BUS Shield](#)
 - [arduino-canbus-monitor](#) - No matter which shield is selected you will need your own sniffer. This is implementation of standard Lawicel/SLCAN protocol for Arduino + any MCP CAN Shield to use with many standard CAN bus analysis software packages or SocketCAN

- [CANtact](#) - "The Open Source Car Tool" designed to help you hack your car. You can buy one or make your own following the guide here.
- [Freematics OBD-II Telematics Kit](#) - Arduino-based OBD-II Bluetooth adapter kit has both an OBD-II device and a data logger, and it comes with GPS, an accelerometer and gyro, and temperature sensors.
- [ELM327](#) - The de facto chipset that's very cheap and can be used to connect to CAN devices.
- [GoodThopter12](#) - Crafted by a well-known hardware hacker, this board is a general board that can be used for exploration of automotive networks.
- [USB2CAN](#) - Cheap USB to CAN connector that will register a device on linux that you can use to get data from a CAN network.
- [Intrepid Tools](#) - Expensive, but extremely versatile tools specifically designed for reversing CAN and other vehicle communication protocols.
- [Red Pitaya](#) - Replaces expensive measurement tools such as oscilloscopes, signal generators, and spectrum analyzers. Red Pitaya has LabView and Matlab interfaces, and you can write your own tools and applications for it. It even supports extensions for things like Arduino shields.
- [ChipWhisperer](#) - A system for side-channel attacks, such as power analysis and clock glitching.
- [HackerSDR](#) - A Software Defined Radio peripheral capable of transmission or reception of radio signals from 1 MHz to 6 GHz. Designed to enable test and development of modern and next generation radio technologies.
- [Carloop](#) - Open source development kit that makes it easy to connect your car to the Internet. Lowest cost car hacking tool that is compatible with SocketCAN and can-utils. No OBD-II to serial cable required.
- [CANBadger](#) - A tool for reverse-engineering and testing automotive systems. The CANBadger consists of both hardware and software. The main interface is a LPC1768/LPC1769 processor mounted on a custom PCB, which offers two CAN interfaces, SD Card, a blinky LED, some GPIO pins, power supply for peripherals and the ethernet port.
- [CANSPY](#) - A platform giving security auditors to audit CAN devices. It can be used to block, forward or modify CAN frames on the fly autonomously as well as interactively.
- [CANBus Triple](#) - General purpose Controller Area Network swiss army knife and development platform.

- [USBtin](#) - USBtin is a simple USB to CAN interface. It can monitor CAN busses and transmit CAN messages. USBtin implements the USB CDC class and creates a virtual comport on the host computer.
- [OpenXC](#) - OpenXC is a combination of open source hardware and software that lets you extend your vehicle with custom applications and pluggable modules. It uses standard, well-known tools to open up a wealth of data from the vehicle to developers. Started by researchers at Ford, it works for all 2002 and newer MY vehicles (standard OBD-II interface). Researchers at Ford Motor Company joined up to create a standard way of creating aftermarket software and hardware for vehicles.
- [Macchina M2](#) - Macchina 2.0 is a complete overhaul of our 1.X generation of Macchina. The goals are still the same: Create an easy-to-use, fully-open, and super-compatible automotive interface.
- [PandwaRF](#) - PandwaRF is a pocket-sized, portable RF analysis tool operating the sub-1 GHz range. It allows the capture, analysis and re-transmission of RF via an Android device or a Linux PC. Capture any data in ASK/OOK/MSK/2-FSK/GFSK modulation from the 300-928 MHz band.

Software

Overview of software, both open source and proprietary, as well as libraries from various programming languages. [This article](#) goes through many of the options below.

Applications

Software applications that will help you hack your car, investigate it's signals, and general tinkering with it.

- [Wireshark](#) - WireShark can be used for reversing CAN communications.
- [Kayak](#) - Java application for CAN bus diagnosis and monitoring.
- [UDSim](#) - GUI tool that can monitor a CAN bus and automatically learn the devices attached to it by watching communications.

- [RomRaider](#) - An open source tuning suite for the Subaru engine control unit that lets you view and log data and tune the ECU.
- [Intrepid Tools](#) - Expensive, but extremely versatile tools specifically designed for reversing CAN and other vehicle communication protocols.
- [O2OO](#) - Works with the ELM327 to record data to a SQLite database for graphing purposes. It also supports reading GPS data. You can connect this to your car and have it map out using Google Maps KML data where you drive.
- [CANToolz](#) - CANToolz is a framework for analysing CAN networks and devices. It is based on several modules which can be assembled in a pipeline.
- [BUSMASTER](#) -An Open Source tool to simulate, analyze and test data bus systems such as CAN, LIN, FlexRay.
- [OpenXC](#) - Currently, OpenXC works with `Python` and `Android` , with libraries provided to get started.
- [openpilot](#) - openpilot is an open source driving agent that performs the functions of Adaptive Cruise Control (ACC) and Lane Keeping Assist System (LKAS) for Hondas and Acuras.
- [openalpr](#) - An open source Automatic License Plate Recognition library written in C++ with bindings in C#, Java, Node.js, Go, and Python.
- [metasploit](#) - The popular metasploit framework now supports Hardware Bridge sessions, that extend the framework's capabilities onto hardware devices such as socketcan and SDR radios.
- [Mazda AIO Tweaks](#) - All-in-one installer/uninstaller for many available Mazda MZD Infotainment System tweaks.
- [mazda_getInfo](#) - A PoC that the USB port is an attack surface for a Mazda car's infotainment system and how Mazda hacks are made (known bug in the CMU).

Libraries and Tools

Libraries and tools that don't fall under the larger class of applications above.

[Custom Applications SDK for Mazda Connect Infotainment System](#) - A micro framework that allows you to write and deploy custom applications for the Mazda Infotainment System.

C

- [SocketCAN Utils](#) - Userspace utilities for SocketCAN on Linux.
- [vircar](#) - a Virtual car userspace that sends CAN messages based on SocketCAN

C++

- [High Level ViWi Service](#) - High level Volkswagen CAN signaling protocol implementation.

Python

- [CANard](#) - A Python framework for Controller Area Network applications.
- [Caring Caribou](#) - Intended to be the *nmap of vehicle security*.
- [c0f](#) - A fingerprinting tool for CAN communications that can be used to find a specific signal on a CAN network when testing interactions with a vehicle.
- [Python-CAN](#) - Python interface to various CAN implementations, including SocketCAN. Allows you to use Python 2.7.x or 3.3.x+ to communicate over CAN networks.
- [Python-OBD](#) - A Python module for handling realtime sensor data from OBD-II vehicle ports. Works with ELM327 OBD-II adapters, and is fit for the Raspberry Pi.

Go

- [CANNiBUS](#) - A Go server that allows a room full of researchers to simultaneously work on the same vehicle, whether for instructional purposes or team reversing sessions.
- [CAN Simulator](#) - A Go based CAN simulator for the Raspberry Pi to be used with PiCAN2 or the open source [CAN Simulator board](#)

JavaScript

- [NodeJS extension to SocketCAN](#) - Allows you to communicate over CAN networks with simple JavaScript functions.

Companies and Jobs

Companies and job opportunities in the vehicle security field.

- [UberATC](#) - Uber Advanced Technologies Center - info@uberatc.com.
- [Tesla](#) - Tesla hires security professionals for a variety of roles, particularly securing their vehicles.
- [Intrepid Control Systems](#) - Embedded security company building tools for reversing vehicles.
- [Rapid7](#) - Rapid7 does work in information, computer, and embedded security.
- [IOActive](#) - Security consulting firm that does work on pentesting hardware and embedded systems.

Coordinated disclosure

- [General Motors](#) on HackerOne - Coordinated disclosure submissions accepted
- [Fiat Chrysler Automobiles](#) on Bugcrowd - Coordinated disclosure submissions accepted, paid bounties offered
- [Tesla Motors](#) on Bugcrowd - Coordinated disclosure submissions accepted, paid bounties offered

Other Awesome Lists

List of lists.

- Security
 - [Application Security](#)
 - [Security](#)

- [Capture the Flag](#)
- [Malware Analysis](#)
- [Android Security](#)
- [Hacking](#)
- [Honeypots](#)
- [Incident Response](#)
- Meta
 - [awesome](#)
 - [lists](#)

Contributing

Your contributions are always welcome! Please take a look at the [contribution guidelines](#) first.

