

Forum: [Hack Forums](#)

Thread: [\[Direct Links\] The Car Hackers Handbooks and Attack Guides](#)

Hazzahx - February 8, 2020, 4:40 pm

Here's some of my favorite books todo with Vehicle Hacking or Manipulation. First off 'The Car Hackers Handbook' this is my goto for anyone wanting to learn anything todo with Vehicle Networks.

This book outlines the very basics to advanced examples that different security manufacturers use and outlines attacks people have used. This also list 'tools of the trade' and many other helpful tools you could use to Penetration test. I'd highly suggest purchasing a hard copy. This is some of my absolute favourite reads but I have plenty more if you're interested.

THE CAR HACKER'S HANDBOOK.

A Guide for the Penetration Tester

by Craig Smith.

<http://opengarages.org/handbook/ebook/>

"The Car Hacker's Handbook describes, in meticulous detail, how your car's components talk both to one another and to diagnosticians—outlining all the ways good and bad guys can modify or attack the systems."

—The Wall Street Journal

How To Hack And Upgrade Your Car Using Can-Bus.

This document is aimed at those unfamiliar with CAN bus or the reverse engineering process, it will cover some very basic and advanced concepts.

<https://www.instructables.com/id/How-to-Hack-and-Upgrade-Your-Car-Using-CAN-Bus/>

Gone in 360 Seconds Hijacking with Hitag2

By Flavio D. Garcia

An in depth look Hitag2 and five common attacks.

https://www.researchgate.net/publication/235916472_Gone_in_360_Seconds_Hijacking_with_Hitag2

Automatic Reverse Engineering of CAN Bus Data Using Machine Learning Techniques.

"we show that reverse engineering of CAN bus traffic is at least partially possible by applying machine learning techniques and the performance of the classifiers increases when adding additional features to the analysis."

https://www.researchgate.net/publication/320837400_Automatic_Reverse_Engineering_of_CAN_Bus_Data_Using_Machine_Learning_Techniques

The Use of CAN Bus Message Electrical Signatures for Automotive Reverse Engineering.

"This paper describes a process that allows the user to identify which CAN messages are transmitted by a particular ECU. This is achieved by getting the electrical signature of each CAN message and matching known CAN messages with unknown ones."

<https://www.kvaser.com/use-can-bus-message-electrical-signatures-automotive-reverse-engineering/>

Also if your interested in Vehicle Hacking feel free to message to join my small group. Thanks