Instead of buying books or paying exorbitant amount of money to learn about car hacking, we (Charlie Miller and Chris Valasek) decided to publish all our tools, data, research notes, and papers to everyone for FREE! Feel free to reach out if you have any questions. If you're nice enough we may actually send you one of our IDBs ;)

Required Reading

Autosec

These fine researchers were the ones that kicked off the car hacking revolution. Without them, we wouldn't have even considered this area of research. Big ups!

The Menu

Adventures in Automotive Networks and Control Units (aka car hacking)

Our orignal work that covered CAN bus sniffing, injection, and attacks against a Toyota Prius and Ford Escape. All our tools and data!

Car Hacking for Poories

Car hacking for poories covers how to get ECUs working outside of the vehicle and use the tools from our first project to inspect CAN bus messages and perform attacks. Also, go carts.

A Survey of Remote Automotive Attack Surfaces

We go over the attack surface of modern connected cars, focusing on entry points and automotive network arechitecture. Some have covered this as the 'most hackable car', but in reality it was just a precursor to our next project...

Remote Compromise of an Unaltered Passenger Vehicle (aka The Jeep Hack)

Most of our research lead up to this point. We hacked a car over cellular for physical control. Charlie and Chris: 1, World: 0. Focus on every aspect of car hacking from CAN bus attacks to reverse engineering ECU firmware. A++ would do business with again.

Advanced CAN Message Injection

So now you know how to pick out a car and remotely hack it. Good for you. Want to do something a bit cooler than change the speedometer? We did too. This paper covers how to setup and control advanced technology features within a vehicle via the CAN bus (such as steering). WARNING: Contains real car hacking achieved via firmware reverse engineering. Open at your own risk.