List of potentially vulnerable cars

At last year’s Defcon, hackers Charlie Miller and Chris Valasek showed how they had managed to manipulate a Ford Escape and a Toyota Prius with nothing more than a laptop and a CAN dongle (and a lot of time – 10 month). For this year’s Black Hat they analyzed the schematics of 24 different car makes and models.

They were looking for possible vulnerabilities that car hackers might be able to explore. As a result they presented a list of cars and the potential hackability of their networked components. In their paper they claim that “some ECUs (Electronic Control Units) communicate with the outside world as well as the internal vehicle network. These ECUs pose the biggest risk to the manufacturer, passenger, and vehicle.” According to the two hackers, their “results aren’t definitive assertions about security vulnerabilities in cars and trucks so much as warnings of potential weaknesses.”

Valasek, who is the director of vehicle security research at the security consultancy IO-Active, described their project such: “For 24 different cars, we examined how a remote attack might work. It really depends on the architecture: If you hack the radio, can you send messages to the brakes or the steering? And if you can, what can you do with them?”

The researchers worked on the underlying principle that more advanced cars are easier to hack than cars with less computer-controlled features: “While all vehicles may (or may) not be vulnerable to safety critical actions through CAN message injection, we assume those with advanced computer controlled features are more susceptible since they are designed to take physical actions based on messages received on the internal network.” The Toyota Prius for example has a collision prevention system that was designed to stop the vehicle when certain CAN messages are received. While this was worked in as a safety feature, it might also present a vulnerability that hackers could explore.

The paper “Survey of remote attack surfaces”, which the researchers published alongside their presentation, lists the 2014 Jeep Cherokee, the 2015 Cadillac Escalade, and the 2014 Infinity Q50 as the most hackable cars on their list. As least hackable they rated the 2014 Dodge Viper, Audi A8, and Honda Accord. The Audi is used as an example for a strong network layout: its wireless features are separated from the driving functions in the internal network. A gateway blocks commands sent from any compromised radio. The Infinity Q50 on the other hand has a network whose radio and telematics components are directly connected to the engine and braking system.