Remote control via the entertainment system

Security researchers have again taken over a car – this time from 16 km away. While the two automobile hackers previously had to directly connect to the CAN network to hack the car, they have now found a way to control it remotely.

TWO YEARS AGO, CHARLIE MILLER AND CHRIS VALASEK published a white paper titled “Adventure in automotive networks and control units”. In it, they describe how they manipulated a Ford Escape and a Toyota Prius. The hackers reengineered the diagnostic interface and injected related messages to the CAN-based in-vehicle networks by means of a laptop and a CAN dongle.

For last year’s Black Hat conference, 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. The 2014 Jeep Cherokee, the 2015 Cadillac Escalade, and the 2014 Infinity Q50 were the most hackable cars on their list.

Working from there, they have now demonstrated that they can in fact hack a Jeep Cherokee without ever touching the car. Journalist Andy Greenberg of Wired has reported how the hackers took over the control of a Jeep he was driving – while they were sitting in Miller’s basement 16 km away. According to Greenberg, “the result of their work was a hacking technique – what the security industry calls a zero-day exploit – that can target Jeep Cherokees and give the attacker wireless control, via the Internet, to any of thousands of vehicles. Their code is an automaker’s nightmare: software that lets hackers send commands through the Jeep’s entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.”

While the account of Greenberg’s drive on the highway in a externally controlled car is quite funny (“As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That’s when they cut the transmission.”), it also quite worrying, especially for anyone driving a Jeep Cherokee. According to the report, the hackers were also able to control the Jeep’s brakes and accelerator.

“All of this is possible only because Chrysler, like practically all carmakers, is doing its best to turn the modern automobile into a smartphone. Uconnect, an Internet-connected computer feature in hundreds of thousands of Fiat Chrysler cars, SUVs, and trucks, controls the vehicle’s entertainment and navigation, enables phone calls, and even offers a Wi-Fi hot spot. And due to one vulnerable element, which Miller and Valasek won’t identify until their Black Hat talk, Uconnect’s cellular connection also lets anyone who knows the car’s IP address gain access from anywhere in the country.”

The attack then turns to a chip in the car’s head unit – the hardware for its entertainment system – rewriting the chip’s firmware to plant the code. That rewritten firmware is capable of sending commands through the car’s CAN network to its physical components like the engine and wheels. It has taken Miller, a security engineer at Twitter, and Valasek, Director of Security Intelligence at IOActive, three years of tearing vehicles apart, mapping their ECUs, and learning how to handle the CAN protocol to get to this point.

The hackers have shared their research with Chrysler, which is why a patch for the Jeep Cherokee is already available. Customers can download the patch from Fiat Chrysler’s website, but it must be implemented via a USB stick or by a mechanic. Ten other Fiat Chrysler models that are equipped with the 8,4-inch touchscreen system are also vulnerable and need the patch. Miller and Valasek will demonstrate a remote attack against an unaltered Jeep Cherokee at next month’s Black Hat USA 2015 conference.