How Hackable Is Your Car? Consult This Handy Chart

Traffic jam, Beijing, China

Stuart Dee/Getty

Last year, when hackers Charlie Miller and Chris Valasek showed they could hijack the steering and brakes of a Ford Escape and a Toyota Prius with nothing but laptops connected to the cars, they raised two questions: Could hackers perform the same tricks wirelessly, or even over the Internet? And even more pressing: Is your specific car vulnerable, too?

If you own a Cadillac Escalade, a Jeep Cherokee or an Infiniti Q50, you may not like the answer.

In a talk today at the Black Hat security conference in Las Vegas—and an accompanying 92-page paper—Valasek and Miller will present the results of a broad analysis of dozens of different car makes and models, assessing the vehicles' schematics for the signs that hint at vulnerabilities to auto-focused hackers. The result is a kind of handbook of ratings and reviews of automobiles for the potential hackability of their networked components. "For 24 different cars, we examined how a remote attack might work," says Valasek, director of vehicle security research at the security consultancy IOActive. "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?”

Miller and Valasek are quick to disclaim that their results aren’t definitive assertions about security vulnerabilities in cars and trucks so much as warnings of potential weaknesses. In contrast to their 2013 research, they didn’t do any hands-on hacking. In fact, their recent work consisted mostly of signing up for mechanics’ accounts on the websites of all the carmakers, downloading the cars’ technical manuals and wiring diagrams, and analyzing the computer networks those documents revealed. “We wanted to take a step back and look at a whole range of cars in much less detail, to really see what was out there,” says Valasek.

In the two researchers’ analysis, three vehicles were ranked as “most hackable”: the 2014 models of the Infiniti Q50 and Jeep Cherokee and the 2015 model of the Cadillac Escalade. The full results, summarized in the chart below, show that the 2010 and 2014 Toyota Prius didn’t fare well either.

A summary of Miller's and Valasek's findings: a plus sign indicates "more hackable," a negative sign "less hackable."

Miller and Valasek's findings represented in a single chart. A plus sign represents "more hackable," a minus sign "less hackable." Credit: Charlie Miller and Chris Valasek

All the cars’ ratings were based on three factors: The first was the size of their wireless “attack surface”—features like Bluetooth, Wi-Fi, cellular network connections, keyless entry systems, and even radio-readable tire pressure monitoring systems. Any of those radio connections could potentially be used by a hacker to find a security vulnerability and gain an initial foothold onto a car’s network. Second, they examined the vehicles’ network architecture, how much access those possible footholds offered to more critical systems steering and brakes. And third, Miller and Valasek assessed what they call the cars’ “cyberphysical” features: capabilities like automated braking, parking and lane assist that could transform a few spoofed digital commands into an actual out-of-control car.

The Infiniti Q50 in particular was a model of insecure architecture, the two researchers say. The sports sedan’s wireless features included remote keyless entry, Bluetooth, a cellular connection, wireless tire pressure monitoring, and an Infiniti Connection system that interfaces with a “personal assistant” app on the driver’s smartphone. Miller and Valasek say that within the Q50’s network, those radio and telematic components were directly connected to engine and braking systems. And the sedan's critical driving systems had computer-controlled features like adaptive cruise control and adaptive steering that a hacker could potentially hijack to physically manipulate the car.

Jeep's 2014 Cherokee didn't rate much better, with many of those same wireless features plus a Wi-Fi network, and even more automated driving features like parallel parking assistance that could potentially be triggered at high speeds. "It’s awesome that it has all these features," says Miller. "But it’s a little scary that they can all talk to each other."

The researchers point to Audi's A8, by contrast, as an example of a strong network layout. Its wireless features were separated from its driving functions on its internal network, with a gateway that would block commands sent to steering or brakes from any compromised radios.

In a statement to WIRED, Infiniti spokesperson Kyle Bazemore responds to the researchers' findings by pointing out that Miller and Valasek didn’t actually hack a Q50. But he writes that the company is nonetheless examining the researchers’ conclusions. “As the potential for ‘hacking’ into the electronic systems of all automobiles may grow, we will continue to integrate security features into our vehicles to help protect against cyber-attacks,” adds Bazemore.

Neither Toyota nor GM immediately responded to a request for comment. A spokesperson for Chrysler wrote in a statement that the company will "endeavor to verify these claims and, if warranted, we will remediate them." The company also took a jab at Miller and Valasek for not sharing their research with the companies before going public with their findings: "We support the responsible disclosure protocol for addressing cyber security threats. Accordingly, we invite security specialists to first share with us their findings so we might achieve a cooperative resolution. To do otherwise would benefit only those with malicious intent."

Miller and Valasek counter that they've shared their report with the Department of Transportation and the Society of Automobile Engineers, an industry group. Their goal is to use public pressure—and if necessary, shame—to push car companies to think about their security architecture.

The possibility of car hacking, after all, is becoming more real; In some cases the researchers analyzed car models over time to see how they were becoming more digitized and thus potentially more insecure. Infiniti, for instance, more than tripled the number of electronic control units (ECUS) in its Q50 between 2006 and 2014; Jeep and Range Rover both more than doubled them between 2010 and 2014. Meanwhile cars are increasingly connected to smartphones and the Internet, in some cases integrating into their dashboards Web browsers that are well-known targets for hackers. "Our main takeaway is that companies should consider security before adding pieces onto an automobile, especially when those pieces have remote connectivity or cyberphysical attributes," says Valasek.

Miller and Valasek also recommend automakers think about more actively foiling hackers. For their talk, the hacker duo has created a prototype of an intrusion detection system for cars–a $150 device that plugs directly into a vehicle's network to monitor and block suspicious commands.

The two researchers, whose earlier work was funded with a grant from DARPA, aren't the first to examine the wirelessly hackability of cars. In 2010 a team of researchers from the University of Washington and the University of California San Diego showed they could take over a car via a smorgasbord of wireless vulnerabilities. Their attack points included the car's Bluetooth connection, its OnStar-like cellular radio, a rogue Android app on the driver's phone synched to the car's network, and even a malicious audio file burned onto a CD in the car's stereo.

But those hackers wouldn't name the car they tested. Miller and Valasek, since the beginning of their auto-hacking exploits, haven't been so discreet.

"You can grab a Consumer Reports magazine from a newsstand right now and see ratings for car safety features," says Valasek. "We're doing the same thing, but for vehicles' cybersecurity."

Read their full paper below:

Survey of Remote Attack Surfaces by Andy Greenberg