**With Wireless Cars, Our Physical Safety Is Now on the Line**

**The march of progress always takes a toll.**

Oct 2015

[By AARON ROBINSON](http://www.caranddriver.com/search/all/author/AARON+ROBINSON)

|  |
| --- |
|  |

From the November 2015 issue *Car and Driver*

There’s an argument to be made that mankind should have stayed in the trees, because progress is a dangerous business. No matter how carefully you engineer a new invention and study the way test subjects use it and build in safeguards against accidental harm or malicious intent, if you start sales on Monday, by Wednesday there will be blood. The act of ­creation produces destruction, which produces improvement, which produces a different kind of destruction, which produces more improvement until, eventually, everybody accepts that even with things that have extensive instruction manuals and a wallpaper of warning stickers and that are widely ­considered perfectly safe, somebody always gets hurt. Were it otherwise, there would be no personal injury lawyers.

Back in 2012, I wrote a column entitled “[Google is my co-pilot. What can go wrong?](http://www.caranddriver.com/columns/aaron-robinson-autonomous-cars-are-upon-us-thanks-to-google-what-can-go-wrong)” In it, I observed that the high-tech industry plunges forward on a relentless pace of invention that generates more than its share of Version 1.0s that are easily hacked and/or don’t work worth a damn. I warned that the same industry now wants to automate your car. Judging from the reader responses, in which I was called “oblivious” and a “sour puss,” not everyone is dreading self-driving cars or giving much thought to the track record of the industry that is pushing them.

Okay then, how many of you want to send your kids off to school in Google Car 1.0? Anyone? History proves that some casualties from a new technology are unavoidable. But there are people who are trying to do something about it. In all likelihood, their actions will save lives.

Charlie Miller and Chris Valasek are computer hackers, an anonymous, cowardly profession not normally associated with laudable deeds. However, these two work on the security side and have applied their talents to new cars, viewing them not as automobiles but as wirelessly connected computer networks with license plates. [In 2013](http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/), they sat in the back seats of a 2010 Ford Escape and a Toyota Prius and, sending computer commands through the onboard diagnostics ports, ordered the cars to commit all kinds of antisocial behavior, including steering off the road and disabling the brakes. Of course, writes *Wired* magazine reporter Andy Greenberg, the hackers had to gain access to the car first, not a very realistic scenario.

|  |
| --- |
|  |
|  |

But Miller and Valasek weren’t finished. This past July, [in a follow-up Wired feature and video](http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/), they showed how they could remotely hack a 2014 Jeep Cherokee from 10 miles away, exploiting a weakness in the car’s Uconnect system, which runs on the Sprint mobile network. While relaxing on the sofa in Miller’s St. Louis living room, the duo took control of the machine with a laptop and a cellphone, turning on and off various systems and putting up a picture of themselves in tracksuits on the car’s center display. Eventually, they shut down the Jeep on a freeway while Greenberg, the team’s panicky test bunny, tried to avoid a serious accident.

Flamers slammed Miller and Valasek for risking innocents by conducting their mayhem on public roads, which is a legitimate beef, but the stunt got people’s attention. Indeed, it made the national news, and Fiat Chrysler Automobiles, which until then had been quietly offering a ­system patch that would have closed the loophole that allowed the hack, suddenly found itself in the glare of the media spotlight and recalled 1.4 million vehicles for software upgrades. Nothing jolts an auto company like a costly recall, especially one prompted by headlines.

Despite industry assurances of firewalls and “air gaps” that isolate the car’s core systems, Miller and Valasek proved that the race to incorporate wireless connectivity is creating entry points for bad guys into the car’s vital systems. It’s no different than when you plugged in your first modem and went from being a private citizen in Anytown, USA, to a target visible to a global cadre of evil nerds who screw up lives for fun or profit. Now your car’s steering, gas pedal, and brakes are on the web.

There is no absolute protection except to stay offline or off the road. The list grows longer of large institutions, those with budgets for serious internet security, that have been hacked silly. This past summer, the federal government had to admit that the personal information of 22 million people, including federal employees, was swiped.

It’s not just our credit cards and Social Security numbers at risk; with wireless cars, our physical safety is now on the line. Miller and Valasek like to release the details of their software breeches at hackers’ conventions. By feeding the wolves, they hope to spur the disorganized and perhaps naïve auto industry to unify and take the threat seriously, and also get more hackers out there trying to find the bugs.

Despite these efforts, the history of invention proves that some casualties are all but certain as cars go wireless and, someday, fully automated. Lawyers will always have work. But I, for one, sleep ­better knowing that at least a couple of those dudes with laptops are on our side.