Should all connected cars have a physical network kill switch?

Aurich Lawson / Getty

reader comments

114 with 79 posters participating, including story author

Share this story

Connected cars should come with a kill switch. That’s the take-home message—and the title—of a report by the group Consumer Watchdog. Software increasingly defines the vehicles we drive, and software can be exploited by nefarious people for nefarious means. The problem is compounded by the fact that automakers rely on software written by third parties, including open source software that is riddled with security holes, it says.

Therefore, to prevent “a 9/11-like cyber-attack on our cars,” the report calls for physical “kill switches” to be built into new cars to allow them to be completely disconnected from the Internet. If carmakers don’t agree to the report’s recommendations by year’s end, then “legislators and regulators should mandate these protections,” it says.

Yes, there’s a modem in your new car

You may have noticed that it’s becoming increasingly difficult

to buy a new vehicle that doesn’t feature an embedded modem in it. The benefits of a connected car are various, we’re told. It enables onboard telematics that the car maker can use both to improve future products and to allow features like predictive maintenance alerts. And an Internet connection to the infotainment system opens up streaming media services alongside more traditional platforms like FM or satellite radio. In Europe, an onboard modem that can call emergency services in the event of a serious crash has been mandatory since last year.

Depending on the car, you can do a lot more. I’m pretty sure every battery-electric vehicle has a smartphone app that lets you control charging and climate settings. And many more cars (with all kinds of powertrains) have apps that let you monitor and even geofence a car. Some new cars have APIs that are accessible to services like Alexa, and an industry-wide fascination with AI is driving digital assistants and of course autonomy itself. All of this is enabled by wireless connection to the outside world, and it involves some pretty deep hooks into the innards of a car—stuff like the brakes, for instance.

Unfortunately, much of the basic internal network that connects the different bits of a car—called a CANbus—was set in stone in the mid-1990s. And much like the cyberpunk fiction of the period, no one really grasped that everything was about to go wireless. As we’ve learned ever since, if you connect a system to the Internet and you don’t make it secure, someone can come along and hack it.

Consumer Watchdog’s report explains this in great depth. It quotes Linus Torvalds on why Linux should never be trusted with a nuclear power station and explains some potential methods of attacking a connected car. It details car hacks of the past such as the infamous Miller and Valasek Jeep hack, and it reprints excerpts from investor communications from companies like Tesla and GM that acknowledge the risks a

hacking incident could cause to the company share price.

But the report is curiously ill-informed on some matters and positively misguided in others. And the picture it paints of the industry—as secretive and sleepwalking into danger—doesn't really reflect the state of the industry as it is today.

"When we talk about the car, I think what's interesting is that the OEMs and tier one suppliers have taken security very seriously," said John Wall, SVP at Blackberry and head of its QNX activities. "If I look back three or four CESes past, there was a lot of emphasis on autonomous drive. Then the Jeep hack happened. It changed the industry overnight. The next year at CES, everybody was coming to us and asking us, "OK, we know you have an ASIL-D certified product. We know you know how to do Functional Safety. What's your security story?" Companies went out and bought security companies. I mean, some of the reaction was knee-jerk," he told Ars. "But the point was, people were taking it seriously. I don't know that they exactly knew. I mean, the reality is, if you look at the Jeep hack, this wasn't a sophisticated hack. This was 'the doors were left wide open,'" Wall said.

Modern cars have modern security on them

As Wall noted, the Jeep hack was possible because the point of entry—its infotainment system—was developed before anyone thought it would one day be connected to the Internet. "The only way you could break into that head unit was physically. At that point, who cares? I mean, if you're inside the vehicle, you can do whatever you want, but then they added a module to it. And suddenly, you had a connected unsecured device. So the first step was for a lot of the OEMs to look at their current crop of devices and say, 'OK, what are the steps we need to take to at least close the open doors?'"

“Putting in passwords, encryption, Secure Boot—all these different things have followed. But now what we’re actually seeing in the industry is the architecture of the vehicle itself is changing. And we’re seeing things like gateways get put into place, separating non-safety buses from safety buses. So there’s a lot of effort going into re-architecting the vehicle from how the buses are actually connected through to issuing certificates for modules that need to authenticate; the level of sophistication is getting much higher,” Wall told Ars.

All of that sounds sensible, but not to Consumer Watchdog. The report gives modern connected device security scant mention beyond a throwaway paragraph on gateways, which it says are “responsible for ensuring only authorized communication can reach the safety-critical systems. While this would seem to solve the problem, it really only adds more complexity. A successful attack must pass through the gateway unit, requiring a more sophisticated attack. However, the additional hardware and software in the gateway unit also create more opportunities for hackers to find vulnerabilities.”

If you have to flip a kill switch in your own car, it’s too late

As an observer of the industry over the past few years, I have to agree with Wall’s assessment—the Jeep hack certainly woke everyone up. When we launched our car section in 2014, it was extremely difficult to get any OEM to talk about the topic of cybersecurity. These days, car companies like GM will even let journalists like me meet their Red Teams, who spend their days finding creative ways to compromise new systems before the cars are unleashed on the public. There’s an Auto-ISAC, where the industry meets to share threat intelligence. And there has been a proliferation of cybersecurity companies pitching their services to the auto industry, with more than a few acqui-

hires.

And even as the automotive threat surface expands, we've yet to see much evidence of malicious actors targeting cars. Why bother going after a car for a bitcoin or two when you could ransomware some hospitals, 23 Texas local agencies, Georgia's court system, Baltimore City government, or a Chinese shipping company? In fact, the only automotive ransomware event we've covered in the past few years was a WCry infection at one of Honda's Japanese factories.

If criminals want to ransom cars, they'll do it by going after someone who can afford to pay them, and that means the OEMs, not end users. And in turn, any kill switches need to be (and indeed are) at that level. Because by the time a driver realizes she needs to turn off the Internet connection to her compromised car, it's already too late. Sadly, most of the recommendations in the Consumer Watchdog report are similarly well-meaning but misguided; I'm not sure the authors would get any industry to agree that "CEOs… should sign personal statements and accept personal legal liability for the cybersecurity status" of whichever company they asked, other than perhaps an actual cybersecurity company. But if the aim was to get people talking about a topic that has very low public consciousness, it might have worked.

https://arstechnica.com/?p=1587835