

Can Your Car Be Hacked?

A Fear That's More Hype Than Reality — for Now

A downside of our Internet-connected lifestyle is that the bits of data and personal information we access online (from finances to Facebook posts) potentially can be viewed by others, without our consent and without us knowing until it's too late. The hacking of connected devices such as computers and smartphones has become common, and no one is immune. No amount of security software and measures can keep hackers at bay if they want to break in badly enough.

Now that cars are becoming connected, they are also vulnerable to hacking. A [recent segment](#) on *60 Minutes* focused on cars, and the challenges of securing connected devices. It showed how a vehicle could be remotely hacked, causing the driver to lose control of essential functions such as braking. The day after the segment aired, U.S. Senator Ed Markey (D-Mass.) [released a report](#) concluding that automakers are not doing enough to secure connected cars and called for creating a federal rating system similar to the one for [crash tests](#) so consumers could assess the cybersecurity level when shopping for a new vehicle.

How real is the threat of connected-car hacking? How could it occur? Is there anything car buyers can do to protect themselves? And what are automakers doing to keep connected cars secure? Here are some answers that separate the scare stories from the real situation.

SEE EDMUNDS PRICING DATA

Has Your Car's Value Changed?

Used car values are constantly changing. Edmunds lets you track your vehicle's value over time so you can decide when to sell or trade in.



Year

Make

Model

See pricing history

Car Hacking: More Hype Than Reality

To date, there's been only [one incidence](#) of car hacking, and that was an inside job by a former car dealership employee in Texas who had access to a system that allows the repossession of cars by disabling the ignition system or honking the horn to embarrass owners who are behind on loan payments. Most other documented car hacks, including the one on *60 Minutes*, were performed by researchers, primarily as part of the Pentagon's Defense Advanced Research Projects Agency's (DARPA) work in the area of cybersecurity.

Nevertheless, "it's becoming a really big concern," says [Thilo Koslowski](#), who covers auto technology for the consulting firm Gartner. "I do expect that some companies may take this too lightly, and this could lead to some very bad news for the auto companies and consumers."

"Cars themselves are not designed to fend off modern cyberattacks," adds Andreas Mai, director of [Smart Connected Vehicle](#) at Cisco Systems. But Mai, along with another automotive software engineer, a car security researcher and an analyst interviewed all say that while cars are just as vulnerable as any other connected device, the recent news reports surrounding car hacking are more hype than reality at this point.

Remote Hacks Are Feasible

While the researchers featured on *60 Minutes* didn't reveal how they gained access to hack the vehicle, which was masked to keep it from being identified by make and model, experts interviewed believe they had physical access to the car via its onboard diagnostic port (OBD-II). This is the port that mechanics plug into to determine the status of a vehicle and detect problems, and that's a way of accessing a car that's consistent with [another high-profile project](#) funded by DARPA. In that case, a pair of researchers tapped into a car's onboard OBD-II port to take control of the brakes, acceleration and other critical systems.

According to Damon McCoy, an assistant professor in the computer science department at George Mason University, the hack seen on *60 Minutes* "replicated and extended, in some ways, our original research," which McCoy conducted alongside colleagues from the University of Washington as part of work by the Center for Automotive Embedded Systems Security (CAESS). The CAESS team said in its published findings that it wanted to "discover [whether] remote exploitation is feasible" and reported that the team was also able to gain access to the vehicle's electronics "via CD players, Bluetooth and cellular radio."

McCoy said that while CAESS found remote hacks are feasible, he added that, "the resources required...are much steeper" compared to being hard-wired into the vehicle via the OBD-II port. "They require a much larger scale of reverse-engineering effort to find those types of vulnerability."

Isolating Critical Safety Systems

Even if a hacker does gain access to a vehicle either by hard-wiring into the OBD-II port or accessing it wirelessly, a car's electrical system is designed to prevent breaching of critical systems.

The electronic architecture of cars today is such that it's "exceptionally difficult to do the levels of hack that some people are envisioning," says John Ellis, formerly global technologist at Ford and now head of the consultancy firm Ellis & Associates. "Safety critical systems — the brakes, the engine, the powertrain — are isolated," he says. "They don't intercommunicate."

Ellis adds that this segregation of critical systems predates car connectivity, and that this electronic architecture, known as the Control Area Network (CAN), was designed "from a safety standpoint, not a cybersecurity standpoint." But as cars get more connected, and as more benefits are delivered via connectivity these barriers will eventually break down, according to Mai.

"Today's vehicle networks are designed in a way so that mission-critical systems are segregated from non-critical mission systems," Mai says. "But at the same time, if you want to take advantage of the benefits that vehicle connectivity brings, like retrieving diagnostic data from a car or providing over-the-air [software] updates, then you need to overcome these physical boundaries.

"So it is somewhat of a Catch-22 to leave these traditional ways of protecting a vehicle behind in order to enable what people are expecting from vehicles in the future," he says.

Other research topics

Research

Buying

Leasing

Sell my car

News

Maintenance

Auto Insurance

Safety

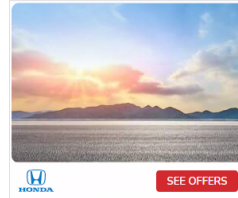
Fuel Economy

Driving Tips

Technology

How To

Advertisement



Advertisement



Ad removed. [Details](#)

Advertisement



Ellis agrees that cars could become more vulnerable to hacking as they become more connected and as automakers rush to add features in order to stay competitive and keep pace with consumer electronics.

"The biggest concern I have is the speed and adoption by automakers of technologies such as over-the-air software updates" that are prevalent in other connected devices, he says.

But these same over-the-air ([OTA](#)) software updates can also be used to plug holes in the security of a connected car, as BMW recently proved. ADAC, the German equivalent of the American Automobile Association, recently found that it was possible for a hacker to [lock and unlock](#) a BMW's doors by communicating with the embedded SIM card that provides the cellular connection for BMW's ConnectedDrive system. The issue affected about 2 million BMW vehicles, but the automaker quickly fixed the problem by pushing out an over-the-air security patch.

Only a few automakers are currently performing over-the-air software updates. But with embedded connectivity coming to more cars, experts say the capability will be used more prevalently for everything from fixing security flaws to handling recall repairs. "One reason [GM introduced 4G LTE](#) in its vehicles is to do OTA updates," says Mark Boyadjis, a senior analyst of automotive infotainment for IHS Technology. Other automakers are outfitting cars with high-speed wireless connectivity for the same purpose, he adds.

No Profit Motive

While it's clear that if you build a connected device, hackers will soon come and try to compromise it, some question whether they'll be inclined to go after connected cars. Currently, there's no strong monetary incentive. "The driver of hacking activities is profit," says McCoy.

Mai adds that such attacks are typically targeted at account information such as credit cards because they are "essentially where the money is."

"This isn't yet prevalent in connected vehicles," he says. "So I would regard vehicles as a lower-priority target for hackers."

If you're still concerned about car hacking, the best way to avoid it is to buy a vehicle with [little to no connectivity](#), but that is becoming more and more difficult. McCoy points out that there are downsides to taking a Luddite approach.

"If you really are concerned about car hacking, I think you'd have to make a lot of trade-offs if you wanted to mitigate these threats," he says. As an extreme example, he points out that an owner could unplug the control unit for a telematics system like [OnStar](#). "But that's a poor trade-off because you're giving up a lot of safety since that unit is more likely to save your life when you get into a crash than cause you to become targeted by a hacker."

The same applies to a car's safety systems. "I think a lot of things that hackers could potentially use against you are things that are much more likely to offer you enhanced safety, like ABS braking," McCoy says. "Sure, a hacker could take control of your ABS system, but the overwhelming odds are that the braking system is going to keep you safe most of the time."

Taking the Issue More Seriously

If there's an upside to the intense and recent focus on car hacking, it's that it has made automakers take cybersecurity more seriously. General Motors, for example, recently hired a [chief product cybersecurity officer](#), the first in the auto industry.

"I think we're talking about the issue before it's a real threat to most drivers on the road," McCoy says. "I hope by talking about it now it will prevent it from becoming a larger issue," and the industry can address problems before they get out of control.

The early warnings are beneficial "to get people to be diligent about this," Ellis adds. "But the problem is nowhere near this cataclysmic event that people keep seeing in the media."

 Edmunds Recommends

Find out what your car is really worth

[Appraise My Car](#)

[Sell My Car](#)

Get a free Edmunds appraisal report for your car in minutes

Year 	Make 	Model 	Go
--	--	---	----

Share:    



Photo Sponsored By
2025 Polestar 3
[Discover Now on Polestar.com](#)



Photo Sponsored By
Visit the Kia Alternative Fuel Showroom
[Learn More >](#)

Save as much as \$2,331 with Edmunds

Select Make

Toyota 

Select Model

RAV4 Prime 

Pricing near

 20001



SE

2.5L 4cyl gas/electric plug-in hybrid CVT

Edmunds suggests you pay



XSE

2.5L 4cyl gas/electric plug-in hybrid CVT

Edmunds suggests you pay

\$43,377

Compare Dealer Prices

\$46,579

Compare Dealer Prices

1 for sale in 20001

What Shoppers Are Searching For

Popular New Cars

Toyota Corolla Cross Hybrid
Toyota Grand Highlander Hybrid
Kia Sportage Hybrid
Volvo EX30
Toyota RAV4 Plug-In Hybrid
Honda CR-V
Volvo XC60
Toyota Highlander Hybrid
Audi Q4 Sportback e-tron
Subaru Crosstrek
Subaru Forester

Toyota RAV4 Hybrid
Honda Pilot
INFINITI QX50
Mazda CX-50
GMC Sierra 2500HD
Lexus NX
Subaru Ascent
Toyota Crown Signia
Kia Sportage Plug-In Hybrid
Subaru Outback
Hyundai Elantra Hybrid
Nissan Titan XD

Popular Used Sedans

Used BMW 5 Series
Used Chevrolet Impala
Used Chevrolet Malibu
Used Chrysler 200
Used Dodge Charger
Used Ford Fusion
Used Ford Taurus
Used Honda Accord
Used Honda Civic
Used Hyundai Elantra
Used Hyundai Sonata

Used Mazda CX-5
Used Nissan Rogue
Used Subaru Crosstrek
Used Subaru Forester
Used Tesla Model X
Used Volvo XC90

Popular Used Pickup Trucks

Used Ford F-150
Used Nissan Titan
Used Toyota Tacoma

Popular Used Hatchbacks

[See more](#)

Join Edmunds

Receive pricing updates, shopping tips & more!

[Back to Top](#)

Email Address

Sign Up

Follow Us



Download the Edmunds app



[Contact Us](#) [Careers](#) [Your Ad Choices](#) [Privacy Statement](#) [Visitor Agreement](#) [Accessibility](#) [Do Not Sell or Share My Personal Information](#) [Edmunds Information](#)

© Edmunds.com, Inc., a wholly owned subsidiary of CarMax, Inc. By using edmunds.com, you consent to the monitoring and storing of your interactions with the website, including by an Edmunds vendor, for use in improving and personalizing our services. See our [Privacy Statement](#) for details.

2025 PROLOGUE SPECIAL APR

0.99%

For well-qualified buyers. Example: 10% down payment, 60 months financing at 1.1% (36month per \$4,000 financed).

SEE OFFERS

Offer ends

2025 Honda Prologue

The all-electric Honda Prologue.

LEARN MORE