

BREAKING NEWS

The leaders of China and Taiwan to meet Saturday for first time since governments split in 1949
(<http://www.wsj.com/articles/china-taiwan-presidents-poised-for-historic-meeting-1446583881>)

THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <http://www.djreprints.com>.

<http://www.wsj.com/articles/hackers-show-they-can-take-control-of-moving-jeep-cherokee-1437522078>

TECH

Hackers Show They Can Take Control of Moving Jeep Cherokee

Using a wireless communications system, researchers manipulate the SUV's electronics

By **DANNY YADRON** and **MIKE SPECTOR**

July 21, 2015 7:41 p.m. ET

Two computer-security researchers demonstrated they could take control of a moving Jeep Cherokee using the vehicle's wireless communications system, raising new questions about the safety of Internet-connected cars.

Fiat Chrysler Automobiles NV, owner of the Jeep brand, on Tuesday blasted the researchers for disclosing their ability to hack into the sport-utility vehicle's software and manipulate its air conditioning, stereo controls and control its speed by disabling the transmission from a laptop many miles away.

The hackers, one of whom works for Twitter Inc. and is a former analyst for the National Security Agency, counter they are bringing attention to an issue auto makers have for too long ignored.

Nearly all modern automobiles, not just those manufactured by Fiat Chrysler, feature computer controls that are potential targets for hackers.

The problem has caught the attention of most major car companies. General Motors Co., for example, has been working with the National Highway Traffic Safety Administration on ways to protect the loads of data that a vehicle carries, and fortify a

car's control system from outside tampering.

Auto executives generally admit the industry is behind in tackling car cybersecurity. Consulting firm Booz Allen Hamilton is pushing them to develop common security measures.

RELATED

The
Jeep

- Luxury Auto Makers Near Deal for Nokia's Maps (<http://www.wsj.com/articles/german-car-makers-audi-bmw-and-daimler-to-buy-nokia-here-1437493575>)

manufacturer, in touch with the hackers for months, released a software patch last week that it said can fix the security flaw. Consumers must either take their vehicle to a dealership or use a USB stick to obtain the update.

The cyberattack demonstration comes amid concerns over how susceptible U.S. automobiles are to hackers taking control of vehicles or accessing motorists' private information. Other researchers next month plan to show how they can hack a Tesla Motors Inc. vehicle.

Tesla said members of its security team would attend a conference in Las Vegas to discuss its security, but it isn't making a vehicle available to hackers. Last year, it sent a manager to the Def Con hacker convention in Las Vegas to recruit hackers to test its vehicles.

It isn't clear how many vehicles are affected by the Jeep security flaw. Fiat Chrysler this year through June 30 sold more than 105,000 Jeep Cherokees, according to Autodata Corp. The researchers believe their hack would work on any late 2013, 2014 or early 2015 vehicle with Fiat Chrysler's Uconnect system.

"Under no circumstances does FCA condone or believe it's appropriate to disclose 'how-to information' that would potentially encourage, or help enable hackers to gain unauthorized and unlawful access to vehicle systems," the auto maker said in a statement.

The two hackers, Charlie Miller, a Twitter employee based in St. Louis, and Chris Valasek, a director at the security firm IOActive, demonstrated in an article and video published in technology magazine Wired their ability to wirelessly access a vehicle's systems. The researchers, who have been probing vulnerabilities in connected automobiles for years, previously could only take over a car by hacking from a laptop

connected by cable to a moving vehicle.

Mr.

WSJ.D

WSJ.D is the Journal's home for tech news, analysis and product reviews.

- [Apple Watch Sales: What We Know \(and Don't Know\)](http://blogs.wsj.com/digits/2015/07/21/apple-watch-sales-what-we-know-and-dont-know/) (<http://blogs.wsj.com/digits/2015/07/21/apple-watch-sales-what-we-know-and-dont-know/>)
- [Sony Is Swooping Into the Drone Market for Business Customers](http://www.wsj.com/articles/sony-to-enter-drone-market-for-business-customers-1437557475) (<http://www.wsj.com/articles/sony-to-enter-drone-market-for-business-customers-1437557475>)
- [Alibaba Unveils Plan to Protect Cloud Data](http://www.wsj.com/articles/alibaba-unveils-plans-to-protect-cloud-data-1437538354) (<http://www.wsj.com/articles/alibaba-unveils-plans-to-protect-cloud-data-1437538354>)
- [How Strong Is Apple's Grip Over Mobile Phones?](http://www.wsj.com/articles/how-strong-is-apples-grip-over-mobile-phones-1437577877) (<http://www.wsj.com/articles/how-strong-is-apples-grip-over-mobile-phones-1437577877>)

Miller defended releasing the information, arguing he is improving auto safety by drawing attention to the issue. “We both want the same thing, to keep drivers safe from a cyberattack,” said Mr. Miller, who used to work on hacking tools for the NSA. “All I can do is point out flaws in their vehicles, get other researchers working on this issue and make suggestions.”

Messrs. Miller and Valasek have kept some of the flaws they uncovered under wraps to prevent copy cats from wreaking havoc on the highway. But they do show in a video that they can effectively disengage a car's transmission or, when it is moving at slower speeds, its brakes. The two researchers say they will show more details during a talk at the Black Hat hacker conference next month.

In February, staff for Sen. Edward Markey (D., Mass.) released a report claiming that nearly all cars and trucks on U.S. roads feature wireless technology prone to hacking or privacy intrusions. The report queried more than a dozen manufacturers in light of studies demonstrating how hackers can infiltrate vehicles to gain control of steering, braking and other functions. The report also raised concerns about companies sweeping up information from navigation systems and storing data with third parties.

Sens. Markey and Richard Blumenthal (D., Conn.) on Tuesday introduced legislation that would require NHTSA officials and the Federal Trade Commission to develop standards for securing vehicles and protecting consumers' privacy.

The legislation would also create a “cyber dashboard” ratings system to inform consumers how well a vehicle protects against hackers.

“Drivers shouldn’t have to choose between being connected and being protected,” Sen. Markey said in a statement. “We need clear rules of the road that protect cars from hackers and American families from data trackers.”

—*Mike Ramsey contributed to this article.*

Write to Danny Yadron at danny.yadron@wsj.com and Mike Spector at mike.spector@wsj.com

Copyright 2014 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.