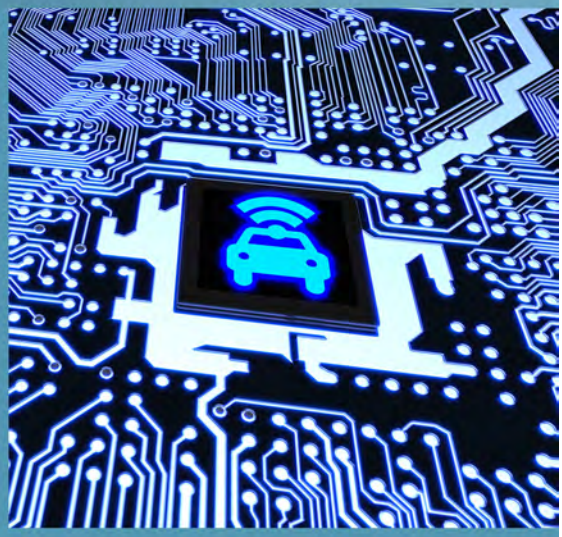
November 2020

CONNECTED CAR REPORT 2020:

THE MODELS MOST OPEN TO HACKS



Consumer Watchdog

All 10 of the top-selling 2020 car models are clearly connected online to safety critical systems and cannot be disconnected, leaving automobiles vulnerable to an unprecedented, large-scale hack, according to a new finding by the nonprofit group Consumer Watchdog.

The advocacy group reviewed technical specifications and surveyed dozens of sales departments and service technicians at major car manufacturers.

All of *Car and Driver*'s top 10 best-selling cars for 2020 clearly have features that allow Internet connectivity with safety critical systems and no known way to disconnect those systems.

Consumer Watchdog also found that many dealership employees misrepresented that critical safety systems of top selling models are linked online and the dangers of such connections.

The report follows revelations by Consumer Watchdog and car industry technologists over the unaddressed perils of security systems in "connected cars."

Sales departments, the pivotal link to the public about a car's performance, were ill-informed about whether critical systems of the car were accessible from outside the vehicle, leaving them prone to hackers. A critical component is often the vehicle's CAN bus, or Controller Area Network, which links the car's critical components, such as brakes and engines, and can be accessible to hackers through a cellular or satellite connection. Many salespersons and service technicians surveyed by Consumer Watchdog said they were not familiar with the component, or misrepresented it and said it wasn't connected to the Internet.

In most cases, the advertised capabilities of the car–for example, the ability to start the engine remotely–proved the point that the cars' safety critical systems were connected wirelessly. Nonetheless, sales representatives misrepresented or obfuscated that connectivity.

Most critically, dealerships said they would not be able to take vehicles offline.

When safety critical systems–brakes, engine, steering–are connected wirelessly there is the possibility of that connection being hacked on a fleet-wide basis. This danger is outlined in Consumer Watchdog's previous report, "Kill Switch: Why Connected Cars Can Be Killing Machines and How To Turn Them Off." (https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19_0.pdf)

To dramatize the fact, with the help of technologists, Consumer Watchdog built a simple box that hijacks a Tesla's cellular connection.

When the Tesla connected to the box, Consumer Watchdog was able to take over the screen of the car and send signals to it, mimicking messages that might come from Tesla. A video of the demonstration can be found here: https://youtu.be/RgpmJ6OhPns

In July 2017, Tesla CEO Elon Musk professed that the biggest danger of autonomous car technology was a "fleet wide hack." In August 2020, it was reported that just months before that 2017 statement Tesla had faced a fleet wide hack, but failed to reveal it to the public or regulators. Instead, it paid the white hat hacker off and kept the incident quiet. Read the story at https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/

The demonstrations reflect the dangers of wireless connections to cars' safety critical systems and the failure of the car industry to create safe designs to deal with it.

The following are findings about popular 2020 models based on *Car & Driver*'s top selling models of 2020.

THE HACK TEN

1: Ford F-150

Wireless Connection To Safety Critical System: **Yes**
Known Method To Disconnect: **No**

Online, dealers advertise the 2020 Raptor as having FordPass Connect, 4G Mobile Hotspot Internet Access, and premium remote start options. The remote start option necessitates a wireless connection to the safety critical systems of the car. If the engine of the car can start remotely, it can be hacked remotely.

Surveyed employees at the Sam Leman Ford in Bloomington, Illinois were not sure if the most popular selling car in the United States was connected online to the car's CAN bus. Kyle, an employee in the sales department, said "the only thing that controls the brakes is the ABS." Morgan, another employee, said SYNC Connect, the vehicle's infotainment system, was linked up to "everything in the truck," allowing owners to start, lock or unlock vehicles at any time. However, he wasn't "too sure about the CAN unit itself."

THE HACK TEN

2: Dodge Ram 1500

Wireless Connection To Safety Critical System: **Yes**
Known Method To Disconnect: **No**

Dodge dealerships advertise the new model as having "smart device integration," "remote engine start" and "UConnect," which allows for remote system updates.

Technologists say these systems necessitate wireless connectivity to safety critical systems.

Employees at Dodge dealerships confirmed there is an app allowing the car to remotely trigger the vehicle's functions, but downplayed insecurity to the vehicle from such a connection.

THE HACK TEN

3: Chevy Silverado

Wireless Connection To Safety Critical System: **Yes**
Known Method To Disconnect: **No**

A member of the service department at Chevrolet Wickstrom named Brody said she was not sure if the Silverado's infotainment system was connected to the CAN bus. The employee pointed to a subscription-based application that goes through Onstar, allowing users to remotely access the vehicle.

Such remote access connections create vulnerabilities to hacks.

Asked if the car could be taken offline, the employee said, "I wouldn't know how to go about. I don't know if we have the capabilities to do something like that."

THE HACK TEN

4: Toyota Rav 4

Internet Connected To Safety Critical System: **Yes**
Known Method To Disconnect: **No**

Online the model doesn't advertise Connected Services, a Toyota infotainment system, or any remote start capabilities

The owner's manual for the 2020 RAV4 describes connected services, including remote access from a smartphone -- though it's not specific about what you can do from the smartphone. The wiring diagram shows a "Telematics Transceiver Assembly" with clear CAN connections to many other systems in the vehicle.

Queries over CAN bus online connectivity to various Toyota dealerships in Illinois turned up mixed responses. "I have no idea what that is," said an employee at Lombard Toyota. Three employees said the car is linked online through Connected Services. "I can almost guarantee if you had Connected Services it would be connected [to the CAN]," said the employee.

Steve Huberty, a member of the Schaumburg Toyota sales team who employees said had a lot of institutional knowledge regarding Toyota manufactured cars, said the upper tier models of the car had remote start capabilities. However, the CAN was not connected to the Internet, according to Huberty. "The car itself is connected to a satellite that creates the downloads. But as far as the Internet it is all wifi based. So unless there is a cellular signal to the car there is no wifi. There is no separate connection to the CAN," he said.

Asked if the model is susceptible to hacking, Huberty said, "At this point in time, no. But I am sure some day they will find out a way." Huberty conflated two issues -- whether passengers can get a wifi (Internet) connection in the car, as opposed to whether hackers with Internet access can gain control of the car's vital systems. The latter may be true even if the connection is via Toyota's servers communicating with the car via satellite.

A Schaumburg Honda dealership said their 2020 model is indeed connected online through HondaLink. “We’re able to connect through the CAN. The infotainment system is connected to that,” said a Honda Schaumburg employee. However, taking it offline is “not something we would do, not something we have heard of.”

Online advertisements for the Rogue SV indicate connectivity features such as remote engine start. Lower models, such as the Rogue S, do not.

Higher end 2020 models have remote start technology but are not connected to the CAN bus, according to a Glendale Nissan employee. The Rogue S, however, doesn't have remote technology, said one employee.

THE HACK TEN

7: Chevrolet Equinox

Wireless Connection To Safety Critical System: **Yes**
Known Method To Disconnect: **No**

A service technician at Leman's Chevy City confirmed that the Internet is connected to the Equinox, including to its CAN bus. "Yes sir, quite a bit tied to that system," said the employee. As for disconnecting online connectivity, he said, "I don't know if it's possible."

The dealership advertised the model as coming with OnStar and Chevrolet Connected Services capabilities.

THE HACK TEN

8: Toyota Camry

Wireless Connection To Safety Critical System: **Yes**
Known Method To Disconnect: **No**

The XSE models have Remote Connect capabilities, while lower models such as the TRD and L do not, according to advertisements.

The connection in the 2020 Camry is very clear from its wiring diagram: two "Telephone" antennas connected to a "Telematics Transceiver" connected to CAN. This is textbook remote access to the car's internal configuration.

Contradicting the wiring diagram, Steve Huberty, salesman at Schaumburg Toyota, said, "The car is not connected to the CAN bus but has remote capabilities triggered by a cellphone, such as remote start."

A Schaumburg Honda service department employee said their 2020 Civic is connected online via the HondaLink infotainment system through the CAN bus. Disconnecting it is not something the dealer would be able to do, according to the employee.

THE HACK TEN

10: Toyota Corolla

Wireless Connection To Safety Critical System: **Yes**
Known Method To Disconnect: **No**

The 2020 model is not connected to the Internet, according to Schaumburg Toyota. Amenities such as remote start won't be offered until 2021 models, according to the dealership.

The wiring diagram for the 2020 Corolla, however, shows two different "Telephone Antennas" -- one on the roof and one in the instrument panel. These connect to a "Telephone Transceiver Assembly" which has a CAN connection. The upper-end 2020 Corolla models have "Safety Connect", "Service Connect", and "Remote Connect" services.

The owner's manual refers to "Toyota Entune Service Connect" which "uses DCM [Digital Communications Module] to collect and transmit vehicle data..." and goes on to list several services. "Service Connect" includes the ability for Toyota to e-mail you "Maintenance Reminders" and "Vehicle Health Reports" based on information gathered digitally from the vehicle, indicating connectivity to the car's the safety critical systems.

GRAND PRIZE:
Tesla, The World's Most Hackable Car

While Tesla's marketing machine makes claims about the security of its connected cars, in August 2020 we learned that three years earlier Tesla's fleet had been hacked and the hacker gained remote access to a safety critical system in every car. This is known as a fleet-wide hack.
(Read the story at https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/)

Jason Hughes hacked Tesla's servers to send "summon" commands to any car, given just its VIN. This meant he could move the cars forward and back a short distance — which is certainly a major safety concern.

The "white hat" hacker informed Tesla, which paid him a $50,000 bounty for the information and fixed it, but the public and regulators were never informed.

TESLA SAFETY CLAIMS

- Engineered to be the safest cars in the world.

- Because every Tesla is connected, we're able to use the billions of miles of real-world data from our global fleet – of which more than 1 billion have been driven with Autopilot engaged – to understand the different ways accidents happen. We then develop features that can help Tesla drivers mitigate or avoid accidents.

- Through over-the-air software updates, we're able to introduce safety features and enhancements long after a car has been delivered, as well as release updated

versions of existing safety features that take into account the most up-to-date real-world data collected by our fleet. https://www.tesla.com/VehicleSafetyReport

FACTS

Tesla's Over The Air (OTA) updates have been hacked and are not safe.

- Consider Keen Labs Tesla Model S hack in 2016, in which they exploited a vulnerability in the over the air update system to take control of the car's brakes, among other things. (See: https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/)

- In spite of Tesla beefing up their cars' security after the 2016 Keen Labs hack, Keen hacked Tesla cars again a year later, which proves that "fixing" a vulnerability doesn't make a car secure; rather, it indicates that the vehicle is not secure by design, demonstrating there are probably more as-yet undiscovered vulnerabilities. (https://electrek.co/2017/07/28/tesla-hack-keen-lab/)

- While OTA updates do have the positive potential Tesla mentioned, it was revealed in 2018 that Tesla abused the OTA update ability to release the Model 3 on an unsuspecting public before the software was fully tested -- knowing they could fix the problem later. That resulted in the May 2018 / Consumer Reports brake fiasco: https://arstechnica.com/cars/2018/05/how-a-software-brake-upgrade-won-tesla-a-consumer-reports-endorsement/

- Later in 2018, there was also a case in which a botched OTA update caused Tesla's Autopilot to stop working, demonstrating that, even without hackers involved, OTA updates can be a liability as well as an asset: https://jalopnik.com/tesla-autopilot-not-working-after-latest-over-the-air-u-1829018937

Tesla uses open source software with serious design deficiencies.

Tesla's cellular connection can be hijacked, as Consumer Watchdog has shown in this new video demonstration: https://youtu.be/RgpmJ6OhPns

Consumer Watchdog is a nonprofit nonpartisan public interest group that has fought for the consumer since 1985. The staff wishes to acknowledge the generous support of the Rose Foundation, which made this project possible.