Automakers trying to prevent hackers from commandeering cars

August 5 2015, byTom Krisher

This product image provided by Fiat Chrysler Automobiles shows the Uconnect 8.4 inch infotainment system on a 2014 Jeep Cherokee Limited. Harman International, the company that makes car radios that friendly hackers exploited to take control of a Jeep Cherokee, on Tuesday, Aug. 4, 2015 said its other infotainment systems don't have the same security flaw. (Fiat Chrysler Automobiles via AP)

When researchers at two West Coast universities took control of a

General Motors car through cellular and Bluetooth connections in 2010, they startled the auto industry by exposing a glaring security gap.

Five years later, two friendly hackers sitting on a living room couch used a laptop computer to commandeer a Jeep from afar over the Internet, demonstrating an even scarier vulnerability.

"Cars don't seem to be any more secure than when the university guys did it," says Charlie Miller, a security expert at Twitter who, along with well-known hacker and security consultant Chris Valasek, engineered the attack on the Jeep Cherokee.

Fiat Chrysler, the maker of Jeeps, is now conducting the first recall to patch a cybersecurity problem, covering 1.4 million Jeeps. And experts and lawmakers are warning the auto industry and regulators to move faster to plug holes created by the dozens of new computers and the growing number of Internet connections in today's automobiles.

The average new car has 40 to 50 computers that run 20 million lines of software code, more than a Boeing 787, a recent KPMG study found.

Miller and Valasek are known as "white hat," or ethical, hackers and reported their findings to the company. But the episode raised the prospect that someone with malicious intent could commandeer a car with a laptop and make it suddenly stop, accelerate or turn, injuring or killing someone.

After the 2010 hack, the auto industry plugged access holes and tried to isolate entertainment and driver information systems from critical functions such as steering and brakes. But in each subsequent model year, it added microchips and essentially turned cars into rolling computers. The introduction of Internet access has created a host of new vulnerabilities.

"The adversary only needs to find one way to compromise the system, where a defender needs to protect against all ways," says Yoshi Kohno, associate professor of computer science at the University of Washington, who was part of 2010 hack.

Mark Rosekind, who heads the National Highway Traffic Safety Administration, has urged the industry to set cybersecurity standards and avoid government regulation.

But two Democratic senators, Edward Markey of Massachusetts and Richard Blumenthal of Connecticut, have introduced a bill that would force the industry to seal off critical computers and add technology to stop hackers in real time.

Security experts say automakers should have systems that recognize rogue commands and stop them from taking control of a car. Some already do. They also say car companies must behave more like the personal computer industry, instantaneously updating software via the Internet to stay ahead in a perpetual cat-and-mouse game. Tesla and BMW already can do this, and nearly all automakers are planning for it.

Even so, experts say it's nearly impossible to stop all cyberattacks, as the U.S. government and major retailers have discovered.

"It's the same thing you see in any industry: You do more and someone finds a way around it," says Bryant Walker Smith, a law professor at the University of South Carolina.

In the 2010 incident, the hackers worked near the car. In the recent Jeep attack, Miller and Valasek used a laptop in Pittsburgh to control the vehicle in St. Louis.

In this July 5, 2015 file photo, motorists guide their vehicles down Interstate 70 through heavy traffic and light rain in Evergreen, Colo. Fiat Chrysler on Wednesday, Aug. 5, 2015 said that it has a software fix that will prevent future hacking into the Jeep Cherokee and other vehicles. (AP Photo/David Zalubowski, File)

They used the Cherokee's cellular connection to access its radio. From there, they penetrated the vehicle's controls, changing its speed and taking over the brakes and the transmission.

Just last week, another hacker revealed that he placed a small electronic box on a car to steal information from GM's OnStar system so he could open doors and start the vehicle. GM said the hack was isolated to one car and it has closed the loopholes.

Miller says Fiat Chrysler did implement some security measures. The hackers at first got to a radio chip that was isolated from critical computers. It took them three months, but they got that chip to talk to another one and give them access to the Jeep's controls. All told, the hack took about a year.

Miller says that because so few people have the expertise and motivation, a large-scale hacking attack on cars is unlikely. "Some teenager is not going to do this or some bored group of undergraduates," he says.

Still, there is reason to question whether the industry is ready for a cyberattack.

Stefan Savage, a computer science and engineering professor at the University of California, San Diego, participated in the 2010 hack. He praised Tesla for hiring a cybersecurity officer with power to make changes. GM created a similar position. But he says other companies he preferred not to name have moved more slowly.

Savage says radios and other devices often have software owned by the outside supplier. As a result, the software can have vulnerabilities an automaker may not know about.

He also says it's difficult to isolate radios, locks and other features from computers that move and stop the car. For instance, after a crash, cars are programmed to unlock their doors.

The Alliance of Automobile Manufacturers, which represents a dozen major companies, says the industry is working with security firms and universities to prevent attacks. Earlier this month, companies formed a group to share information. Some companies such as Audi offer rewards to outside experts who find vulnerabilities in their systems.

Savage predicts all automakers will accelerate plans for instant Internet software updates.

"I'd be shocked if everyone doesn't deploy this stuff in the next few months," he says. "They can't afford not to."

Citation: Automakers trying to prevent hackers from commandeering cars (2015, August 5) retrieved 27 June 2024 from https://phys.org/news/2015-08-automakers-hackers-cars.html