Written by **Joe Wolverton, II, J.D.** on July 22, 2015

# Hackers Seize Control of Jeep Exploiting Vulnerability in Chrysler Cars

Ever wonder if hackers could take control of your car's computer while you were driving down the interstate? One man's recent experience proves they can, and have done so. Here's the amazing (and frightening) story told July 21 by security reporter Andy Greenberg on the Wired website:

> I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.
>
> Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.
>
> As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car's digital display.

Greenberg wasn't the victim of a random cyberattack, however. He was voluntarily participating in "car-hacking research" being conducted by two hackers, Charlie Miller and Chris Valasek. The story continues:

> The result of their work was a hacking technique — what the security industry calls a zero-day exploit — that can target Jeep Cherokees and give the attacker wireless control, via the Internet, to any of thousands of vehicles. Their code is an automaker's nightmare: software that lets hackers send commands through the Jeep's entertainment system to its dashboard functions, steering, brakes, and transmission, all from a laptop that may be across the country.

Greenberg was in on the plan from the beginning and was told exactly which of the car's functions the duo would hijack from Miller's house located about 10 miles from the "attack."

In the aftermath of the demonstration, Chrysler released a software patch for a range of its models (including those manufactured with the Fiat brand) that use a proprietary in-dash Internet interface they call Uconnect.

Rather euphemistically, the announcement on Chrysler's website simply recommended that customers download a "software update to improve vehicle electronic security."

Given how much control Miller and Valasek were able to exercise over Greenberg's Jeep, one would hope the "recommendation" would be a bit more strongly and urgently promoted by the carmaker.

Regarding the Uconnect system's vulnerability, *The Guardian* reported:

> Unlike some other cyberattacks on cars where only the entertainment system is vulnerable, the Uconnect hack affects driving systems from the GPS and windscreen wipers to the steering, brakes

> and engine control.
>
> The Uconnect system is installed in hundreds of thousands of cars made by the FCA group since late 2013 and allows owners to remotely start the car, unlock doors and flash the headlights using an app.

According to the report by *The Guardian*, Miller and Valasek informed Fiat Chrysler of the hole in its Internet interface nine months ago. The software patch was not released by the company until July 16:

> Not only was Fiat Chrysler terribly late in pushing out the fix, customers have to "update their cars by visiting the manufacturer's site, downloading a programme on to a flash drive and inserting it into the car's USB socket."

That kind of customer experience doesn't seem to represent the "caring for people" motto the company proclaims on its website.

While the likelihood of someone experiencing this type of cyberattack is remote (no pun intended), there is a darker dimension to this revelation. Since 2012, stories have leaked detailing the U.S. government's creation and implementation of two cyber attacks on the information systems of other nations.

"Flame" was the name of a computer virus reportedly developed and launched by the United States in order to glean critical data from computers in several Middle Eastern countries.

According to a story published in the *Washington Post*, the United States and Israel launched a joint venture to develop the Flame virus. Once launched into cyberspace, the code reportedly collected online intelligence data that was then used to create a similar bit of malware that would cripple Iran's nuclear capabilities. Officials cited in the *Post* article revealed that the effort was a collaboration of the National Security Agency (NSA), the CIA, and the Israeli military.

One product of that Israeli-American secret enterprise was the Stuxnet virus. Stuxnet was the virus allegedly deployed by the United States to decelerate Iran's progress toward the development of a nuclear weapon.

Apparently, Flame and Stuxnet were just the beginning of a more sophisticated and sustained American cyber assault against the Iranian nuclear infrastructure. As one source quoted by the *Washington Post* reports, "This is about preparing the battlefield for another type of covert action," said one former high-ranking U.S. intelligence official, who added that Flame and Stuxnet were elements of a broader assault that continues today. "Cyber-collection against the Iranian program is way further down the road than this."

Soon after the existence of Flame and Stuxnet was uncovered (some say leaked by the Obama administration itself), the *Post* ran a story claiming that the ultra-secret Defense Advanced Research Projects Agency (DARPA) was preparing to test "unmanned cyber attacks" that launch themselves without the need of a human at the controls.

One former member of the Air Force Judge Advocate General Corps sees the Pentagon's creation of these weapons as the first step toward the deployment of an autonomous weapon that not only launches without human direction, but can choose its own targets as well.

"News reports that DARPA is seeking proposals for methodologies that would automate cyber responses in predetermined scenarios is an almost inevitable development given the speed in which cyberattacks can cause harm," said Charles Dunlap, now a Duke University Law School professor. "The very idea of

autonomous weapons systems of any kind, cyber or kinetic, is controversial on legal, ethical and even pragmatic warfighting grounds. Yet the development and deployment of such weaponry is sure to continue even as we sort out the law and policies to address it."

For its part, the Department of Defense responds that any operations conducted by the government in cyberspace will be used solely for the protection of our national security.

In this era of the all-seeing, all-cataloging, all-powerful surveillance state, is it too far-fetched to imagine a scenario where, in an effort to "protect national security," federal agents at the NSA, the FBI, or Homeland Security exploit the demonstrated deficiencies in these automobile automations?

Imagine an alleged "domestic terrorist" speeding across the country trying to escape government persecution when all of a sudden his car's steering mechanism is remotely hijacked by some snoop with a laptop.

With Trapwire in place, the feds already have real-time access to the millions of surveillance cameras installed from coast to coast and along nearly every interstate and surface street in America. The next step — seizing remote control of the car — would be a snap.

As of press time, Fiat Chrysler Automobiles has made no comment on the demonstration.