GlobalResearch
Center for Research on Globalization

Wireless Carjacking: The Chrysler Recall

By Dr. Binoy Kampmark
Global Research, July 29, 2015
Region: USA
Theme: Global Economy

Caught with their proverbial pants down, Fiat Chrysler executives have issued a voluntary recall of a good 1.4 million cars for the vulnerabilities of its installed internet system. Last Tuesday, Wired burst the bubble of confidence by showing how hackers could take control of a Jeep Cherokee via its internet-connected entertainment system. "Hackers remotely kill a Jeep on the highway – with me in it," wrote correspondent Andy Greenberg.[1]

Channelling, without attribution, Hunter S. Thompson's drug seizure "somewhere around Barstow on the edge of the desert" in *Fear and Loathing in Las Vegas*(1971), Greenberg relates how he was driving at 70 mph "on the edge of downtown St. Louis when the exploit began to take hold." Both cases have a superficial similarity: in either case, an agency of sorts had seized the moment and conquered the human. Either you ingest a good wallop of mind altering substances, or you take the folly-ridden ride on a not so smartphone on wheels.

Charlie Miller and Chris Valasek demonstrated with chilling effect how the vehicle itself could be controlled remotely through a "zero day exploit". (Well, quite literally – the Jeep Cherokee did blast cold air, another remotely executed specialty on the part of the duo.) This entails something akin to a total takeover of the system, one where the dashboard functions, steering, brakes and transmission, may be effectively piloted from a distant source.

The range of vehicles affected by this brazen, and entirely appropriate stunt, is impressive, ranging from the 2013-2015 MY Dodge Viper specialty vehicles to the 2015 Doge Challenger sports coupes. They share the common ground of having 8.4-inch touchscreens. But the bigger picture on connected cars goes beyond this – with 26 million functioning on roads in 2013, the number is projected to rise to 152 million by 2020, at least according to the boffins at IHS Automotive estimates.

The market did not take the results too well, with the stock value of Fiat Chrysler Automobiles dropping by more than 2 percent, with an 8 percent fall in the stock value of Sprint, the cellular network connected with Chrysler's system.

Chrysler and fellow automakers were not operating in the dark on this one. Moving into the land of smartphone technology was always going to come with its automated hazards. Valasek, director of security intelligence at IOActive, had previously engineered a control action over the wheels, brakes, accelerations and displays in a Toyota Prius and Ford F-Escape.

In February, Senator Ed Markey (D-Mass.) was spreading the word via a Congressional report that a mere two out of 16 major automakers "were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real time."[2] And just to dispel any

doubt, the findings of the report are stated as revealing "that there is a clear lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle or against those who wish to collect and use personal driver information." Powerful, and rather damning stuff indeed.

In May, the exercise of questioning the automakers – this time 17 in total – was taken up by the House of Representatives' Energy and Commerce Committee. The letter observed that the use of such connected devices which exacerbated "existing cybersecurity challenges" did also produce a dire prospect: "the threat of physical harm – as products responsible for public health and safety are integrated into the Internet ecosystem."[3]

Responses to such incidents have become scripted affairs, lying in a PR province where fudged accounts and fuzzy justifications hold sway. While the onus should be on the company for allowing such a system to be installed in the first place (wireless entertainment does come first), the emphasis is placed on hacking as a crime, the big dos and don'ts of interacting with the machine. Should anyone entertain the notion, any such behaviour "constitutes criminal action". The response can never be: We told you so.

Then comes the cooling water to douse the flames of recklessness. The company claimed it was "unaware of any injuries related to software exploitation." The recall is packaged in neat terms of consideration, enabling the "ongoing software distribution that insulates connected vehicles from remote manipulation."

While the political classes tend to get distracted by phantoms and hobgoblins, the wireless carjack scenario has been concerning enough to Senators Markey and Richard Blumenthal (D-CT) to warrant action. In Markey's own words, "Drivers shouldn't have to choose between being connected and being protected." Truth is, drivers will increasingly run out of choice in terms of what systems, vulnerable or otherwise, are put in their vehicles.

Legislation would require the National Highway Safety and Transportation Administration and the Federal Trade Commission to jointly create standards on hack-proof vehicle defences with countermeasures and the safeguarding of personal information collected from the vehicle itself (*Wired*, Jul 21).[4]

The last reflection ought to fall on the security experts behind the experiment. In responding to the actions of Chrysler, Miller posed the biting, if logical question on Twitter: "I wonder what is cheaper, designing secure cars or doing recalls?"

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email:bkampmark@gmail.com

Notes

[1] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[2] http://www.marketwatch.com/story/will-car-hacking-become-the-new-carjacking-2014-06-03

[3] http://energycommerce.house.gov/press-release/committee-leaders-seek-information-auto--cybersecurity

[4] http://www.wired.com/2015/07/senate-bill-seeks-standards-cars-defenses-hackers/

Articles by: Dr. Binoy Kampmark