GlobalResearch
Center for Research on Globalization

Hackers Expose New Method For Disabling Vehicles

By Kevin Samson
Global Research, August 12, 2015
Activist Post 11 August 2015

Last month, a massive vehicle recall from automaker Fiat-Chrysler shocked many who were still unaware at the ease of hacking modern-day vehicles. The research covered what is called a "zero-day exploit" hack, which enabled a test vehicle to be fully hijacked simply from obtaining knowledge of the vehicle's IP address.

The main culprit that was addressed by Fiat-Chrysler, which led to the voluntary recall of *1.4 million vehicles*, was any car that came equipped with 8.4-inch touchscreens as part of the vehicle's audio/video system.

Wired writer Andy Greenberg is back today with more information from security researchers who were able to show an even *easier* method to cause a potentially fatal crash in their Corvette test vehicle.

It appears that today's interconnected smart gadgets and modern computing applications are making cars one of the more vulnerable everyday items open to life-changing hacks. Like cutting the brakes….

As you'll see in this video, it only takes a smartphone for an outside operator to take full remote control.

As Greenberg reports:

> At the Usenix security conference today, a group of researchers from the University of California at San Diego plan to reveal a technique they could have used to wirelessly hack into any of thousands of vehicles through a tiny commercial device: A 2-inch-square gadget that's designed to be plugged into cars' and trucks' dashboards and used by insurance firms and trucking fleets to monitor vehicles' location, speed and efficiency. By sending carefully crafted SMS messages to one of those cheap dongles connected to the dashboard of a Corvette, the researchers were able to transmit commands to the car's CAN bus—the internal network that controls its physical driving components—turning on the Corvette's windshield wipers and even enabling or disabling its brakes.
>
> […]The device that the UCSD researchers exploited for those attacks was a so-called OBD2 dongle built by the France-based firm Mobile Devices, but distributed by corporate customers like the San Francisco-based insurance startup Metromile. Metromile, the only one of those corporate distributors whose devices the researchers fully analyzed, is an insurance company that gives its customers the cellular-enabled devices, branded as the Metromile Pulse, to plug into a port on their dashboards as a means of tracking cars and charging drivers on a per-mile basis. The company has even partnered with

> Uber to offer the devices to its contract drivers as part of a discount insurance program. (emphasis added)

Similar to the response by Chrysler-Fiat, the researchers said that once alerted to the problem, the company quickly offered a security patch. However, according to the statements above, Metromile clearly isn't the only distributor. They also used the same deflection as Chrysler-Fiat by saying that no one had reported the issue out in the field. But why wouldn't these companies be properly testing in advance for these vulnerabilities? This is where the problem still remains according to researchers:

> ...the larger problem of wirelessly hackable dongles plugged into cars' networks is far from solved. They say they also notified Mobile Devices of its hardware's insecurity, and were told that the latest versions of the company's dongles weren't vulnerable to their attack. But the researchers nonetheless found in scans of the Internet using the search tool Shodan that in addition to the Metromile device, thousands of still-hackable Mobile Devices dongles were visible, mostly in Spain—possibly those used by the Spanish fleet management firm and Mobile Devices customer Coordina. Mobile Devices hasn't responded to WIRED's request for comment or for a list of its main customers.
>
> [...]the problem is hardly limited to Metromile, Coordina, or even their device supplier Mobile Devices. The insurance company Progressive also offers so-called "telematics-based insurance" using a similar OBD2 plug-in it calls the Snapshot. Earlier this year security researcher Corey Thuen found that the Progressive Snapshot device had its own serious vulnerabilities, though Thuen didn't demonstrate a proof-of-concept attack. And researchers at the cybersecurity firm Argus found that the Zubie, an OBD2 device for personal tracking of driving efficiency, had hackable flaws, too. (emphasis added)

And for those who might feel comfortable that this appears not to be a potentially widespread problem contained with other autos, Wired was quick to point out that it wasn't a Corvette vulnerability, nor something only used in commercial transit:

> ...UCSD researchers say they could have hijacked the steering or brakes of just about any modern vehicle with the Mobile Devices dongle plugged into its dash. "It's not just this car that's vulnerable," says UCSD researcher Karl Koscher. He points to the work of researchers Charlie Miller and Chris Valasek, who revealed and published the code for a wide array of attacks on a Toyota Prius and Ford Escape in 2013 that required only access to a vehicle's OBD2 port. "If you put this into a Prius, there are libraries of attacks ready to use online." (emphasis added)

Hackers are often maligned by media and governments as anarcho-terrorists who aim to bring nothing but disorder and destruction to the world, but fortunately some of them are doing the work that our supposedly trusted corporations should be doing.

This is a story worth paying attention to; it is most assuredly just the tip of the iceberg. It is also a useful topic to offer to those who would knee-jerk shout "conspiracy theory!" when presented with the strange events surrounding the fatal car crash of journalist Michael Hastings, for example.

Perhaps we can now start taking a much closer look at boats, planes, GPS-driven munitions,

unmanned vehicles and even smart homes that also can be taken over via remote control.

And let us take another look back to 2012 when DARPA itself went on record with these very same concerns:

Image Credit: C3 Group, appearing on Forbes

The original source of this article is Activist Post
Copyright © Kevin Samson, Activist Post, 2015

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Kevin Samson

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca