

WHY APPLE SHOULD PAY PARTICULAR ATTENTION TO WIRED'S NEW CAR HACKING STORY

This morning, Wired reports that the hackers who two years ago hacked an Escape and a Prius via physical access have hacked a Jeep Cherokee via remote (mobile phone) access. They accessed the vehicle's Electronic Control Unit and from that were able to get to ECUs controlling the transmission and brakes, as well as a number of less critical items. The hackers are releasing a report [correction: this is Markey's report], page 86 of which explains why cars have gotten so much more vulnerable (generally, a combination of being accessible via external communication networks, having more internal networks, and having far more ECUs that might have a vulnerability). It includes a list of the most and least hackable cars among the 14 they reviewed.

Most Hackable

1. 2014 Jeep Cherokee
2. 2015 Cadillac Escalade
3. 2014 Infiniti Q50

Least Hackable

1. 2014 Dodge Viper
2. 2014 Audi A8
3. 2014 Honda Accord

Today Ed Markey and Richard Blumenthal are releasing a bill meant to address some of these security vulnerabilities in cars.

Meanwhile – in a remarkably poorly timed

announcement – Apple announced yesterday that it had hired Fiat Chrysler’s former quality guy, the guy who would have overseen development of both the hackable Jeep Cherokee and the safer Dodge Viper.

Doug Betts, who led global quality at Fiat Chrysler Automobiles NV until last year, is now working for the Cupertino, Calif.-based electronics giant but declined to comment on the position when reached Monday. Mr. Betts’ LinkedIn profile says he joined Apple in July and describes his title as “Operations-Apple Inc.” with a location in the San Francisco Bay Area but no further specifics.

[snip]

Along with Mr. Betts, whose expertise points to a desire to know how to build a car, Apple recently recruited one of the leading autonomous-vehicle researchers in Europe and is building a team to work on those systems.

[snip]

In 2009, when Fiat SpA took over Chrysler, CEO Sergio Marchionne tapped Mr. Betts to lead the company’s quality turnaround, giving him far-reaching authority over the company’s brands and even the final say on key production launches.

Mr. Betts abruptly left Fiat Chrysler last year to pursue other interests. The move came less than a day after the car maker’s brands ranked poorly in an influential reliability study.

Note, the poor quality ratings that preceded Betts’ departure from Fiat Chrysler pertained especially to infotainment systems, which points to electronics vulnerabilities generally.

As they get into the auto business, Apple and

Google will have the luxury that struggling combustion engine companies don't have – that they're not limited by tight margins as they try to introduce bells and whistles to compete on the marketplace. But they'd do well to get this quality and security issue right from the start, because the kind of errors tech companies can tolerate – largely because they can remotely fix bugs and because an iPhone that prioritized design over engineering can't kill you – will produce much bigger problems in cars (though remote patching will be easier in electric cars).

So let's hope Apple's new employee takes this hacking report seriously.