Experts: Car Hacking Incident Shows Growing Attack Surface, Need To Build In Security

Friday, July 24, 2015 - More and more industries are embracing technology, but security experts said that this week's car hacking incident highlights the need for more emphasis on developing new technologies with a security-first mindset.

On Tuesday, Wired published a report that hackers Charlie Miller and Chris Valasek had successfully hacked into reporter Andy Greenberg's Jeep Cherokee using a zero-day exploit in the car's Uconnect system. In doing so, the hackers gained access to the vehicle's entertainment system, controls, steering, brakes, transmission and more -- from more than 10 miles away -- and ultimately caused the car to crash in a ditch.

As a result, Fiat Chrysler on Friday announced the recall of 1.4 million vehicles for a software patch that should fix the vulnerability. Also, the National Highway Traffic Safety Administration has launched an investigation into the hack.

The event serves as an eye-opener for automakers and others in industries that have started to embrace technologies, said **Mark Mancini, vice president of technology and business development at Fort Lauderdale, Fla.-based JDL Technologies.** While there are many benefits to using technology, there are also vulnerabilities that need to be taken into account, he said.

"Our vehicles are intelligent in ways we didn't even dream about 30 years ago," Mancini said. "They can back up for us, adjust themselves to our profiles, take us to locations we don't know how to get to, tell us when our tires are low, and [have] dozens of other smart functions that make driving easier and in many ways safer. But, our smart cars are as much computer as they are transportation, and we need to think of them as computers, with all that implies."

However, it isn't as simple an answer as launching a recall and a patch every time a vulnerability is found, security experts agreed.

Instead of rushing hot new technology to market and then correcting it when a vulnerability is discovered, this week's car hacking shows that all industries need to change the way they go to market and move toward a security-first development mindset, said Dell's Brett Hansen, executive director, marketing end user computing software and mobility solutions.

"We're already at a point, where, from a technology perspective, just like a PC can be attacked, so can a car," Hansen said. "What we need to think about is: What are the exploits that we need to focus upon to minimize the attack surface and thus reduce risk?"

To start, Hansen said, that means identifying where vulnerabilities are in code that has already been written. But, in the long term, he said, companies will have to be more purposeful when writing code, keeping security in mind and asking themselves what are the worst-case vulnerability scenarios.

"Let's first understand, what are the attack surfaces, what do we need to do to mitigate those? And let's look into those fundamental changes ... to ensure that it's the best-quality code," Hansen said.

Mancini said he was optimistic that car manufacturers and other industries would embrace this security-first point of view in the wake of this recent incident and in preparation for presumably others down the road.

"As soon as the automakers start thinking of their products as computers on wheels, security layers will start to be baked in to the car computer systems and offered in aftermarket tools the same way that firewalls and intrusion prevention systems are provided for computer networks today," Mancini said.

The 'smarter' we get, the smarter we need to get."

Article posted on CRN at: http://www.crn.com/news/security/300077560/experts-car-hacking-incident-shows-growing-attack-surface-need-to-build-in-security.htm

JDL Technologies