FEB 25, 2015 07:02 AM

A- A A+

Car Hacking: How Safe Are You Behind the Wheel in Today's Digital Society?

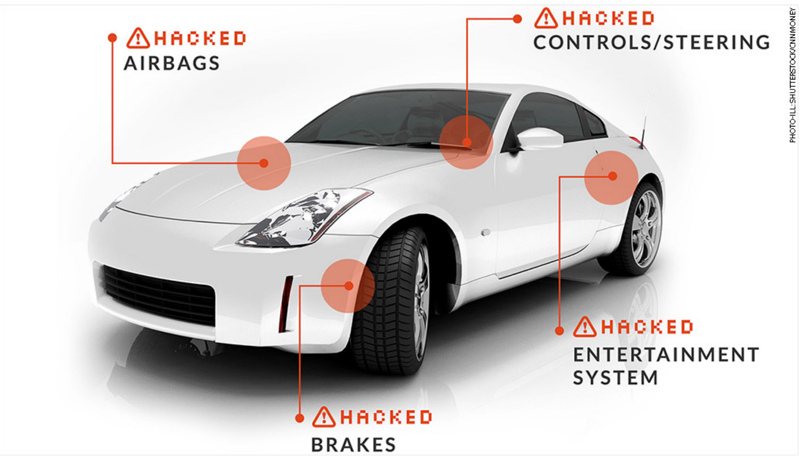
Got those highway blues, can't you hear my motor runnin'
Flyin' down the road with my foot on the floor
All the way in town they can hear me comin'
Ford's about to drop, she won't do no more

By Neal Leavitt

Those were the first four lines from that classic Doobie Brothers song, "Rockin' Down the Highway."

Lead singer Tom Johnston probably never envisioned that someday that car might be flyin' down the road controlled by someone else's digital foot.

Yes, your Ford is now morphing into a giant computer – and it can be hacked.



Last July, for instance, the German ADAC motoring association notified BMW that there was a flaw in BMW's *ConnectedDrive* software – it allows the vehicle to wirelessly transmit/receive data and enables an app to unlock the car via a driver's smartphone.

More than 2 million BMW cars (including Minis and Rolls-Royce) were at risk. BMW was able to quickly develop a vehicle patch, but it wasn't until the second week of December that a fix was finalized.

"The need to get things to market quickly, the constant need to deliver new functionality, is resulting in insufficient attention being paid to make the software trustworthy," said Tony Dyhouse, director of UK-based, government-led Trustworthy Software Initiative.

Report raises startling issues

This was further illustrated a few weeks ago in a report released by U.S. Senator Edward Markey, a member of the Senate Commerce, Science and Transportation Committee. It was based on responses from a bevy of leading automakers, some of which include BMW, Chrysler, Ford, GM, Honda, Nissan, Toyota, and Volkswagen.

Some key findings as reported by *Help Net Security*:

- Most auto manufacturers were unaware of or unable to report on past hacking incidents;
- Security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across different manufacturers;
- Nearly 100 percent of vehicles on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions;
- A majority of automakers offer technologies that collect and wirelessly transmit driving history information to data centers, including third-party data centers, and most didn't describe effective means to secure the information;
- Customers are often not explicitly made aware of data collection and when they are, they often

Latest Posts

Car Hacking: How Safe Are You Behind the Wheel in Today's Digital Society?

Wednesday, Feb 25, 2015

BLOG POST The complexity of today's cars is staggering – being mechanically inclined doesn't cut it these days – you have to be a bit of a computer whiz too in order to service new model cars.

CES a Showcase for Offbeat Gadgets

Wednesday, Jan 28, 2015

BLOG POST This marked my 10th consecutive year at International CES, and as regular as the day's sunset, there will always be on display various gadgets that make you scratch your head and wonder what the inventors were thinking. And with others, you still scratch your head as well and think – what a clever idea! Why didn't I think of that?

High-Tech Ordering Becoming the Norm at Both Mainstream and Fast-Food Restaurants

Monday, Dec 1, 2014

BLOGPOST It's probably not too far fetched now to predict that in the near future – at least within the next decade or so according to some studies and experts – you might be served by R2D2, or a similar robotic food service entity. Yes, numerous restaurants, especially those of the fast-food variety, are rapidly embracing

Classroom Technology Changing the Way Kids –

Computing Now Blogs

Aberdeen Group - A Harte-Hanks Company
Big Data Trends: by David Feinleib
Enterprise Thinking: by Josh Greenbaum
Excelsior College
A Cloud Blog: by Irena Bojanova
Mind the Cloud: by Thoran Rodrigues
Musings from the Ivory Tower by Sorel Reisman

can't opt out without disabling valuable features, such as navigation.

Mechanics need to be computer whizzes

It's a scary scenario. The complexity of today's cars is staggering – being mechanically inclined doesn't cut it these days – you have to be a bit of a computer whiz too in order to service new model cars. *Money* reported, for instance, that "the space ship that put humans on the moon, Apollo 11, had 145,000 lines of computer code. The Android operating system has 12 million. A modern car? Easily 100 million lines of code."

"Auto manufacturers aren't up to speed," added Ed Adams, a researcher at Security Innovation, a company that tests automobile safety. "They're just behind the times. Car software isn't built to the same standards as say, a bank app – or software coming out of Microsoft."

Security measures being bypassed

And Sen. Markey said some security measures used by automakers – ID numbers and radio frequencies – can be identified and rewritten or bypassed.

Granted, there is no known real-world case of a car being hacked remotely – not yet, at least.

But Sean Kane, president of Massachusetts-based Safety Research and Strategies, said there are big concerns about wireless access.

Also, as reported by David Shepardson in the *Detroit News*, "the issue could be even more important as future vehicles communicate with one another through 'vehicle to vehicle' technology to prevent crashes, but could also be at risk of hacking."

Shepardson added that the Society of Automotive Engineers has created a Vehicle Electrical System Security Committee to draft standards that help ensure electronic control system safety. And Sen. Markey wants the National Highway Traffic Safety Administration, working in conjunction with the Federal Trade Commission, to set standards to protect the data, security and privacy of drivers.

Hopefully the automotive industry and ancillary trade/business stakeholder groups will sort this all out sooner, rather than later, and not, to quote a favorite Capitol Hill catchphrase, 'kick the can down the road.'

In the meantime, Edmund King, president of British motoring group The AA, tossed this warning our way:

"You're getting cars that are connected to the Internet 24 hours a day. If cybercriminals target automobiles like they're targeting other things, we'll be in for a hard and fast ride."

Page(s):

Share this:

Please login to enter a comment:

Facebook Google LinkedIn OpenID Twitter Yahoo

Powered by OneAll Social Login

NealNotes: by Neal Leavitt

No Batteries Required: by Ray Kahn

Notes from the Expo Floor: by Brian Kirk

Out of Print: by Evan Butterfield

Rackspace Sponsored Content

Shay Going Mobile: by Shay Shmeltzer

Software Solutions

Software Technologies: by Christof Ebert