Car hack reveals peril on the road to Internet of Things

August 6 2015, by Glenn Chapman

The ability to seize data from and take control of once-dumb devices that are now deemed "smart" with wireless Internet connections was a hot topic at the premier Black Hat cybersecurity conference in Las Vegas

A software glitch that allows hackers commandeer a Jeep Cherokee while on the move is just a glimpse of dangers on the road ahead for the

Internet of Things.

The ability to seize data from and take control of once-dumb devices that are now deemed "smart" with wireless Internet connections was a hot topic at the premier Black Hat cybersecurity conference in Las Vegas Wednesday.

Researchers described how they remotely took control of a moving car or re-aimed high-tech sniper rifles, and many at the gathering warned the ramifications could be far more serious and wide-reaching.

For starters, many companies don't even have teams tasked with making sure their smart devices are secure.

"Almost none of the Internet of Things device-makers have any real security teams, it is sort of a gold rush to market," Black Hat founder Jeff Moss told AFP.

He expects the problem to grow, with skilled hackers eager to push the boundaries.

"The Jeep hack is the beginning," said Moss, who also founded the annual Def Con hacking conference that takes place later this week in Sin City.

"Criminals are geniuses at figuring out how to misuse this stuff."

He theorized a scenario in which a connected home appliance, a toaster for example, is hacked and becomes an entry point for an attack that hops wirelessly to other online devices, such as entertainment systems. A hacker could then jump next door via wireless Internet to take over a neighbor's home devices.

The possibilities for hackers are numerous—and chilling.

Data from smart appliances or other devices can be used to learn about people's lifestyles or daily routines. Cameras in smart gadgets could be activated to spy on intimate moments people would prefer to keep private.

Adding to the problem is the fact that smart appliances, such as ovens or washing machines, are designed to last but do not typically get software updates. With time, hackers find vulnerabilities, and companies do not protect devices against attacks with new security software.

Black Hat founder Jeff Moss told AFP he expects the problem of seizing data from and taking control of devices with wireless Internet connections to grow, with skilled hackers eager to push the boundaries

"You can see us racing toward a future where everything is connected, nothing is updatable, and it is going to last 10 years," Moss said.

"Then, it is a numbers game. A million of anything is trouble, a hundred million is a disaster."

Massive car recall

Fiat Chrysler Automobiles issued a safety recall for 1.4 million US cars and trucks in July after hackers demonstrated that they could remotely control their systems while the vehicles are in operation.

The recall came after cybersecurity experts Charlie Miller and Chris Valasek remotely commandeered a Jeep Cherokee, made by Chrysler, to demonstrate the vulnerability of the vehicles' electronic systems.

Working from laptop computers at home, the two men were able to enter the Jeep's electronics via its online entertainment system, changing its speed and braking capability and manipulating the radio and windshield wipers.

The pair said it was a fairly easy job.

"We might be good at what we do, but this was a weekend project," Miller said.

"What if we did this full time, or got paid to do it?"

Miller is a security researcher at Twitter and Valasek works at cybersecurity firm IOActive.

Fiat Chrysler Automobiles issued a safety recall for 1.4 million US cars and trucks in July after hackers demonstrated they could remotely control their systems while the vehicles are in operation

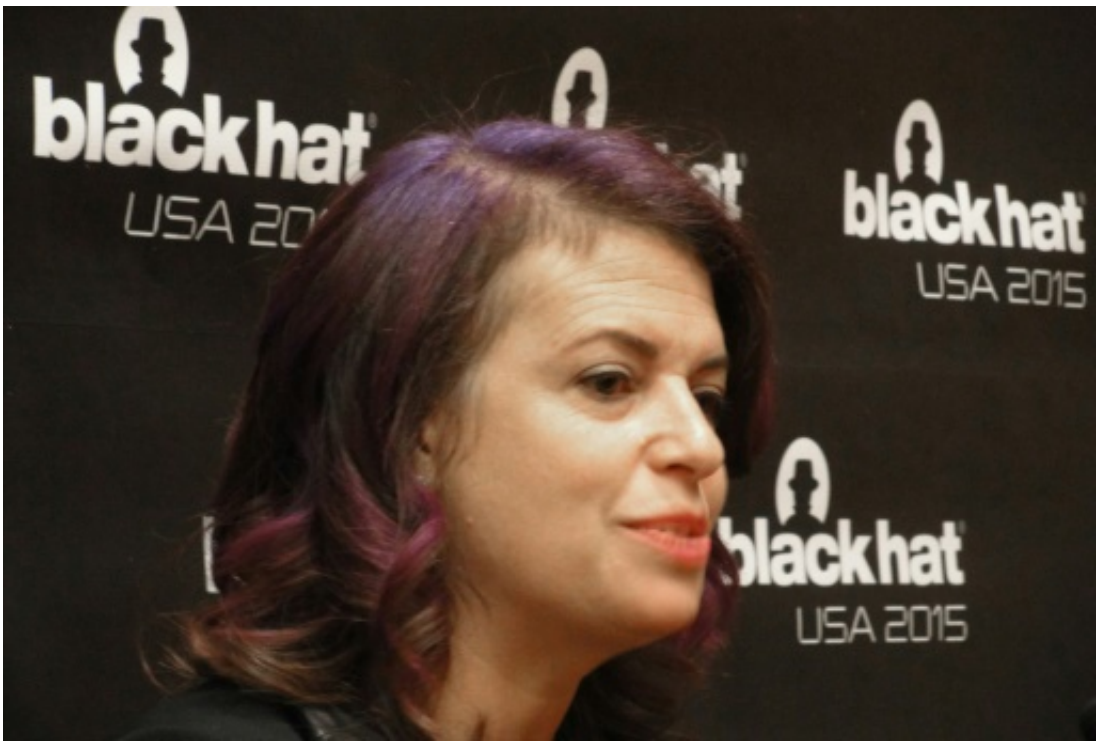
Miller and Valasek said they dug into automobile security because they wanted to make a point.

"Car companies spend millions of dollars on safety, and now this is a part of safety, whether they like it or not," Valasek said.

After the report, Chrysler offered a free software patch for vulnerable vehicles, but said it had no first-hand knowledge of hacking incidents.

The recall involves a broad range of Dodge, Jeep, Ram and Chrysler automobiles produced between 2013 and 2015 that have radios vulnerable to hacking.

The hack involved Harman hardware and the Sprint mobile network, but fixes have been put in place to block the tactic, according to Miller and Valasek.



The Internet of Things promises to spotlight a liability issue software makers have managed to avoid, according to Jennifer Granick, director of civil liberties at the Center of Internet and Society at Stanford University law school

Moss said the potential for hacking Internet-connected power meters was especially troubling. Hackers could not only target individual homes but could cause trouble on city grids, perhaps by toying with electric power in entire neighborhoods.

The Internet of Things promises to thrust into the spotlight an issue of liability that software makers have managed to avoid, according to

Jennifer Granick, director of civil liberties at the Center of Internet and Society at Stanford University law school.

Most people might not think to sue a software maker when a computer crashes, but the odds are high they will when a smart car crashes, Granick said.

"Something that now has software in it but didn't before is going to blow up," added Granick, who gave a keynote presentation at Black Hat.

"Software liability is unavoidable, and it is necessary."