Report: Automakers fail to fully protect against hacking

February 9 2015

In this June 18, 2012 file photo, Sen. Edward Markey, D-Mass., speaks on Capitol Hill in Washington. Automakers are cramming cars with wireless technology, but they have failed to adequately protect those features against the real possibility that hackers could take control of vehicles or steal personal data, according to an analysis of information that manufacturers provided to Sen. Markey. Markey asked automakers a series of questions about the technologies and any safeguards against hackers built into their vehicles. He also asked about how the information that vehicle computers gather and often transmit wirelessly is protected. (AP Photo/J. Scott Applewhite, file)

Automakers are cramming cars with wireless technology, but they have failed to adequately protect those features against the real possibility that hackers could take control of vehicles or steal personal data, a member of the U.S. Senate is asserting.

Basing his argument on information provided by manufacturer, Sen. Edward Markey has concluded that "many in the automotive industry really don't understand what the implications are of moving to this new computer-based era" of the automobile.

The Massachusetts Democrat has asked automakers a series of questions about the technologies—and any safeguards against hackers—that may or may not have been built into the latest models of their vehicles. He also asked what protections have been provided to ensure that information computers gather and often transmit wirelessly isn't used in a harmful or invasive manner.

Appearing Monday on "CBS This Morning," Markey said motorists should be asking questions because "there really aren't any clear guidelines on the books."

Markey said the movement of the automobile from the combustion engine era to the computer era carries wide implications. "No longer do you need a crowbar to break into an automobile," he said in the interview. "You can do it with an iPad."

Markey posed his questions after researchers showed how hackers can get into the controls of some popular cars and SUVs, causing them suddenly to accelerate, turn, sound the horn, turn headlights off or on and modify speedometer and gas-gauge readings.

The responses from 16 manufacturers "reveal there is a clear lack of appropriate security measures to protect drivers against hackers who

may be able to take control of a vehicle or against those who may wish to collect and use personal driver information," a report by Markey's staff concludes.

Today's cars and light trucks typically contain more than 50 electronic control units—effectively small computers—that are part of a network in the car. At the same time, nearly all new cars on the market today include at least some wireless entry points to these computers, such as tire pressure monitoring systems, Bluetooth, Internet access, keyless entry, remote start, navigation systems, WiFi, anti-theft systems and cellular-telematics, the report said. Only three automakers said they still have some models without wireless entry, but those models are a small and declining share of their fleets.

"Americans are basically driving around in computers," Markey said.

Most new cars are also capable of collecting large amounts of data on a vehicle's driving history through an array of pre-installed technologies, including navigation systems, telematics, infotainment, emergency assistance systems and remote disabling devices that allow car dealers to track and disable vehicles whose drivers don't keep up with their payments or that are reported stolen, the report said.

Half the manufacturers said they wirelessly transfer information on driving history from vehicles to another location, often using third-party companies, and most don't describe "an effective means to secure the data," the report said.

Manufacturers are also using personal vehicle data in various and often vague ways to "improve the customer experience," the report said. Policies on how long they store drivers' information vary considerably. Customers often are not made aware explicitly of the data collection and, when they are, they frequently cannot opt out without disabling

valuable features like navigation.

Last November, 19 automakers accounting for most of the passenger cars and light trucks sold in the U.S. agreed on a set of principles to protect motorists' privacy. The voluntary agreement was aimed in part at heading off possible legislation. Markey has said voluntary efforts don't go far enough.

The auto industry is also in the early stages of establishing a voluntary information sharing and analysis center or other comparable program about existing or potential cyber-related threats. "But even as we explore ways to advance this type of industrywide effort, our members already are each taking on their own aggressive efforts to ensure that we are advancing safety," the Alliance of Automobile Manufacturers said in a statement.

The Society of Automotive Engineers also has established a security committee that is evaluating the vulnerability of cars to hacking and is drafting "standards and best practices to help ensure electronic control system safety," the alliance said.

The Association of Global Automakers, another trade association, said the responses provided to Markey are many months old and don't reflect extensive discussions between the industry and federal technology experts aimed at improving the industry's understanding of cyber threats.

The manufacturers who replied to Markey are BMW, Chrysler, Ford, General Motors, Honda, Hyundai, Jaguar Land Rover, Mazda, Mercedes-Benz, Mitsubishi, Nissan, Porsche, Subaru, Toyota, Volkswagen-Audi and Volvo. Three other automakers—Aston Martin, Lamborghini and Tesla—didn't reply to his request for information.