Issued 1/16/18

Car Hacking a Very Real Threat as Autos become ever more Loaded with Tech

Automakers and suppliers are making progress in protecting vehicles from cyber attacks, but the car-hacking threat is still real and could get increasingly serious in the future when driverless vehicles begin talking to each other. A worst-case scenario would be hackers infiltrating a vehicle through a minor device, such as an infotainment system, then wreaking havoc by taking control of the vehicle's door locks, brakes, engine or even semi-autonomous driving features. Such a scenario was shown to be possible in a 2015 remote hacking demonstration involving a Jeep Cherokee that rocked the industry and prompted Fiat Chrysler Automobiles to send UBS sticks with software patches to the owners of 1.4 million cars and trucks. In response to the hacking threat, more vehicles are gaining the ability to wirelessly download security patches, similar to how computers and smartphones have been getting software updates for years. These over-the-air updates allow auto companies to respond to threats — and newly discovered vulnerabilities — faster than having to direct customers to bring their vehicles to dealerships. In years past, well-meaning individuals who pointed out software flaws in vehicles sometimes faced cold receptions or even cease-and-desist letters.

The FCA in 2016 partnered with a San Francisco-based company to launch a "Bug Bounty Program" that pays so-called white-hat hackers up to $1,500 each time they discover a previously unknown vulnerability in vehicle software. The major automakers also created the Automotive Information

Sharing and Analysis Center, known as Auto-ISAC, to research and discuss best practices for cybersecurity. The potential danger of hacking could grow more serious once autonomous vehicles start hitting the roads in significant numbers in the 2020s. These driverless cars will be communicating with each other, through means such as the "Cellular-Vehicle-to- Everything" system that Ford announced last week during the CES tech show it is testing with chipmaker Qualcomm. Justin Cappos, a computer science professor at New York University's Tanden School of Engineering, said one of the more promising ways to stay ahead of hackers is through regular over-the-air software updates to fix vulnerabilities as soon as they become known. For example, Tesla last summer sent out updates to all Tesla Model Xs after Chinese security researchers managed to turn on a Model X's brakes remotely and to get the doors and trunk to open and close while blinking the lights in time to music streamed from the vehicle's audio system