HOW TO KEEP *HACKERS* **OUT** OF THE DRIVER SEAT

by Jenny Mangelsdorf

As automotive manufacturers add more Internet-enabled technology to their vehicles, the risk of unwanted passengers joining the ride grows. From less harmful invasions, where hackers use mobile devices to unlock doors and steal valuables, to more dangerous scenarios where criminals remotely disable a car's systems during operation — today's connected cars are ripe for cyberexploitation.

For many customers, the more bells and whistles — from communications tools to automated parking and driverless capabilities — the better. For manufacturers, innovations can bring better margins along with better brand appeal. However, as new features launch, the vulnerabilities they produce are raising red flags.

"Anybody who's making cars now is looking at smart cars, high tech and making a five-year-out plan, and in those plans, security is becoming more and more of a business issue," says Tom Patterson, CSC Cybersecurity Consulting global managing partner. "Every main auto company now has a senior security executive in place who's talking to … peers and working with the government. Tesla, for example, has been hiring the greatest security brains it can find, outbidding Facebook and eBay, to design better cars."

Much like the Internet's early days, when innovation spread faster than new email connections, the early addition of IT to automobiles seemingly came before manufacturers gave thought to cybersecurity. However, governments have been monitoring the addition of IT to automobiles for at least a decade.

In 2009, Germany launched "Security in Embedded IP-based Systems," an initiative to develop a universal security solution for internal and external vehicle networking based on IP. Recently, the U.S. National Highway Traffic Safety Administration formed an Electronics Council, with cybersecurity as a key topic.

Driving more risk

As new Internet-enabled devices offer to improve safety, traffic flow, and fuel and driver efficiencies, manufacturers will continue to add innovations and drive greater risks to infrastructure, and consumer safety and privacy.

ABI Research estimates that by 2019 more than half, 55.6 percent, of all new vehicles globally will drive off the plant floor already equipped with telematics, which combines telecommunications and informatics. However, security will increasingly dictate auto manufacturers' pace, as more news emerges of successful hacks by researchers of vehicles already on the road.

In 2013, computer security researchers Chris Valasek and Charlie Miller demonstrated they could use a laptop to hack a Ford Escape's and Toyota Prius' systems. A year later, they reported on other vehicles' vulnerabilities; other researchers also report success in remotely hacking vehicles.

Cars, like smartphones, rely on commercial global positioning system (GPS) satellites, yet the integrity of those systems is not guaranteed, says Patterson, noting in a CSO blog post that cheap GPS jammers have been used to disrupt driverless cars, as has the more complex effort of sending false GPS signals to cars.

Manufacturers also are starting to use a controller area network (CAN) protocol to manage communications between devices and a car's systems. However, notes Patterson, security researchers have shown that they can build a $20 CAN hacking tool that takes over a moving car's steering and brakes.

"If a manufacturer or repair shop can take data out of a car for diagnostics, then a criminal can add malware to a car — that interface also presents a key security challenge," adds Paul Scott, CSC Global Automotive industry strategist.

Privacy joins the road

While governments and manufacturers focus on safety, privacy won't take a back seat for long. "In most western countries, data generated by consumers and their cars is designated as the consumer's private property," says Scott. "As manufactures add even more telematics to their cars, or offer them as extras, the data generated by them will pose a bigger security threat."

As other sectors, such as retail and financial services, bear responsibility for protecting consumer data, it's plausible that manufacturers also will be responsible for the risks tied to protecting a driver's private data, especially as they seek to gain financially from the escalating amounts of data generated by connected cars and their drivers — whether simply location data, or car-to-driver, car-to-car or car-to-passenger data.

"Privacy will definitely become an issue, just because of the voluminous nature of the data and the ability now to turn that into gold," says Scott.

In August 2014, a security advocacy group called I am the Cavalry issued a letter to automotive industry leaders asking them to adopt five key capabilities that create a baseline for safety regarding computer systems in cars. The group also developed a petition that lets consumers urge manufacturers to make a commitment to cybersecurity.

Building in security

Manufacturers' recent efforts to improve security can be seen in actions such as the Auto-ISAC, which the Alliance of Automobile Manufacturers, the Association of Global Automakers and leading automotive supplier, Delphi, formed in July 2014, with a plan to establish a cyberthreat and vulnerability information-sharing and analysis center. Simultaneously, cybersecurity specialists continue to challenge manufacturers to increase their efforts, work with standards organizations and learn from other sectors' organizations.

"They should look at collaborative efforts that have worked for other industries, such as the ecosystem the FS-ISAC [Financial Services Information Sharing and Analysis Center] has built to support the security of all of its members," says Patterson. He adds that manufacturers also need to build a cybersecurity framework they can use when building vehicles.

"We're won't have self-driving cars in two years, but we might have them in five, so manufacturers had better get started on building a framework now," says Patterson. "Companies need to be looking at their cars and their supply chains, as well as changes in the ecosystems that they don't control, including infrastructure, such as roads, stoplights and parking meters, and as the 'Internet of Things' drives further connectivity between people and their environments."

To create such an industry framework requires manufacturers to open up some of their intellectual property and use more-open systems. CSC, as other organizations do, uses open source software products in its solutions and actively open sources certain software of its own.

"A manufacturer may have the safest car, but no one will want it if it doesn't function in the real world," says Patterson. "Today, the most secure car on the road could be that 1970s jalopy in the garage, simply because it has no IT in it." ■

JENNY MANGELSDORF is a writer for CSC's digital marketing team.