ITL INSURANCE THOUGHT LEADERSHIP

January 11, 2017

Cybersecurity Holes in Connected Cars

Summary:

A couple of well-chronicled incidents have ratcheted up consumers? anxiety over the possible erosion of control over their cars.

By: *Byron Acohido*

The photo was jarring. A Jeep Cherokee stalled in a ditch after hackers remotely disabled its brakes. No one was hurt. The experiment in St. Louis was a coordinated hackconsumer warning about the possibility of an attacker remotely exploiting vulnerabilities. And cybersecurity issues have come to the forefront in discussions about the pitfalls of the Internet of Things as the technology rapidly evolves. A couple of well-chronicled incidents, including the Jeep, have ratcheted up consumers? anxiety over the possible erosion of control over their cars. The fallout from the Jeep hack, wherein the security experts gained control of the car through its entertainment system, Uconnect, was swift. Chrysler, who owns the Jeep brand, recalled 1.4 million cars to fix the software bug. And Sprint, whose network was used in Uconnect, blocked access to a specific port for the private IP addresses used to communicate with the vehicles. Meanwhile, U.S. Sens. Edward Markey, D-Mass., and Richard Blumenthal, D-Conn., introduced a bill designed to require U.S. cars to meet certain standards of protection against digital attacks and privacy. ?In the rush to roll out the next big thing, automakers have left the doors unlocked to would-be cyber criminals,? Blumenthal said. Art Dahnert, managing consultant at digital security firm Cigital, acknowledges the emerging problem but isn?t overly alarmed. Unless professionally coordinated, the current level of vehicle hacking generally requires close proximity to the car, he says. ?A lot of it is hype,? he says. ?Some of the issues may not affect a lot of consumers.? Still, consumers who own connected vehicles?and most new cars are?should be aware of relevant security risks and developments, he says. Here are some issues to consider.

- **Owner education.** Understanding how a vehicle and some components are connected to the internet is crucial. Cars contain numerous electronic units that control a wide range of functions, ranging from steering and braking to in-car Wi-Fi and diagnostics. These computers are networked and expose possible entry points for hackers. In-car Wi-Fi can

be spoofed or accessed by hackers in nearby locations. And GPS, Bluetooth and smartphones can serve as conduits for hackers wishing to tap into the car?s control system. ?If an app that manages your sound system is compromised, your phone is compromised,? Dahnert says.

- **Updating software.** Software bugs are inevitable. And vehicle owners should be vigilant in keeping up with updates, recalls and service bulletins. Criminals also may exploit update notices by sending fraudulent email that contains malicious software. Avoid downloading software from third-party websites or file-sharing platforms.
- **Limit in-car use.** Some digital bells and whistles are better left turned off whenever possible. ?I would recommend that drivers learn how to disable some of the less used features of the vehicle, especially those that involve remote communications like Wi-Fi hotspots and remote starting,? Dahnert says. ?These steps reduce the footholds that attackers use to hack your car.?
- **Beware of third-party accessories.** More third-party devices, such as insurance dongles, car monitoring tools and other telematics, can be plugged into the vehicle?s diagnostic port and become access points for hackers. Car owners should check with the security and privacy policies of device manufacturers and look to avoid them if they are from obscure companies or deemed untrustworthy. Some accessories also may be problematic. In August, researchers at the University of Birmingham in the U.K. used a piece of radio hardware to intercept signals from a key fob used in Volkswagens. The signals can be replicated to open the doors of millions of Volkswagens dating back to 1995, the researchers claim. ?Don?t forget that it?s not just what?s under the sheet-metal, but what is in your pocket that could lead to a problem,? Dahnert says.
- **Pitfalls of modification.** Avid car owners are notorious for their love of modification, using after-market parts. Those who modify their electronic control units or wireless connections to enhance their cars? performance could be inviting cybersecurity problems. ?Such modifications may also impact the way in which authorized software updates can be installed on the vehicle,? the FBI says.
- **Supplier concerns.** The advent of autopilot cars and driver-assist systems will muddle the already complex ecosystem of car manufacturers and suppliers. Heightened security standards and practices within the connected car supplier ecosystem would be needed as technology evolves, Dahnert says.

Ultimately, consumers have little direct control over the manufacturing and development of the Internet of Things in cars. But they can affect the industry with their checkbooks. ?Consumers need to demand (security features) are updated. Don?t buy products that are not secured,? Dahnert says. *This article originally appeared on ThirdCertainty. It was written by Roger Yu.*

ITL INSURANCE THOUGHT LEADERSHIP

Byron Acohido

byron@thirdcertainty.com

Byron Acohido, one of the nation's most respected cybersecurity and privacy experts, has stepped into a new role: editor-in-chief at IDT911. Acohido first began paying close attention to cybersecurity and privacy in 2004 as a technology reporter and web producer at USA Today.