Report warns of possible mass casualties from automotive cyberattacks

1 August 2019, by Eric D. Lawrence

Credit: CC0 Public Domain

Warnings about connected vehicle vulnerabilities have been a steady drumbeat for years. Now a consumer-advocacy group is putting it in starker terms, suggesting a mass cyberattack against such vehicles could lead to Sept. 11-level casualties.

California-based Consumer Watchdog has issued a 49-page report that paints the dire picture and urges automakers to install 50-cent "kill switches" to allow vehicles to be disconnected from the Internet. The report highlights numerous widely reported instances of remote vehicle hacking, such as a 2015 demonstration involving a Jeep Cherokee left crawling along a St. Louis-area freeway.

"Millions of cars on the internet running the same software means a single exploit can affect millions of vehicles simultaneously. A hacker with only modest resources could launch a massive attack against our automotive infrastructure, potentially causing thousands of fatalities and disrupting our most critical form of transportation," the group warns.

The report highlights what it describes as the key security flaw in connected vehicles, noting that the potential vulnerability is growing because of the increasing number of such vehicles on the roads.

"Experts agree that connecting safety-critical components to the internet through a complex information and entertainment device is a security flaw. This design allows hackers to control a vehicle's operations and take it over from across the internet," the report said, noting that "by 2022, no less than two-thirds of new cars on American roads will have online connections to the cars' safety-critical system, putting them at risk of deadly hacks."

While noting that over-the-air updates—increasingly embraced by automakers—provide the ability to update software, potentially fixing bugs and making a system more secure, the feature could also open new vulnerabilities, the report said. Such over-the-air updates also provide a way to avoid notifying regulators of issues.

The report said various automakers—Tesla, Daimler, Ford, General Motors and BMW, for instance—have disclosed the cyber risks to their investors.

Representatives of the National Highway Traffic Safety Administration, the agency charged with regulating vehicle safety, did not respond to a request for comment.

Gloria Bergquist, a spokeswoman for the Alliance of Automobile Manufacturers, an industry trade group, suggested the report could be an attention-getting ploy, and she defended the industry's cybersecurity efforts.

"It is not unusual to see groups seeking attention right before the August cybersecurity meetings in Vegas. But today, cybersecurity is a priority to every industry using computer systems, including

automobiles. Automakers know their customers care about security, and automakers are taking many protective actions, including designing vehicles from the start with security features and adding cybersecurity measures to new and redesigned models," Bergquist said, referencing an upcoming cybersecurity conference where vulnerabilities found in BMW models are scheduled to be discussed.

Bergquist highlighted various efforts to address the issues, including groups working to develop a unified international standard for automotive cybersecurity. She also said consumers have responsibilities, too.

"Cybersecurity is everyone's responsibility, and consumers—along with automakers and their suppliers—need to be vigilant. Consumers should exercise good cyber hygiene in all they do, including properly pairing a phone to a car, deleting phone data from rental cars (if paired), and being active in doing the maintenance and updates as requested for phones and vehicles," Bergquist said.