Who Pays if Self-Driving Cars Are Hacked?

Experts propose that governments provide manufacturers of autonomous cars with insurance to compensate victims of mass hacking events.

December 7, 2021 By Jeanette L. Pinnace

Driverless cars may one day be commonplace worldwide. But what happens if the software these vehicles use to communicate with one another gets hacked? Study findings published in the journal Computer Law & Security Review show that current motor vehicle insurance isn't enough to cover the potential damage such automobiles might cause, reports a press release from the University of Exeter. What's more researchers suggest that governments might need to come up with novel solutions to compensate those affected by such hacks.

Scientists from Exeter and Sheffield Hallam University in the United Kingdom conducted the study, which focused on potential problems connected with this rapidly expanding technology. Some of the major issues researchers noted included hackers using routine software updates to target vehicles; the danger driverless cars would pose to motorists and others affected by software glitches or hacking threats; and the fact that current systems of financial liability do not apply to autos operated sans drivers.

"It's impossible to measure the risk of driverless vehicles being hacked, but it's important to be prepared," said Matthew Channon, PhD, a law lecturer at Exeter and the lead author of the study. "We suggest the introduction of an insurance backed Maliciously Compromised Connected Vehicle Agreement to compensate low-cost hacks and a government-backed guarantee fund to compensate high-cost hacks. This would remove a potentially onerous burden on manufacturers and would enable the deployment and advancement of driverless vehicles in the U.K."

The insurance industry in the United States has for the past several years focused on various safety issues connected with driverless technology, including determining who is at fault in the case of accidents or deaths.

Some industry experts believe that the manufacturers of these so-called connected and autonomous vehicles will bear the lion's share of responsibility among insurers, technology suppliers of artificial intelligence (AI), car owners and municipalities.

Earlier this year, the European Union Agency for Cybersecurity offered insights on cybersecurity challenges connected with autonomous driving.

“The increased uptake of AI technologies has further amplified this issue with the addition of complex and opaque ML algorithms, dedicated AI modules and third-party pretrained models that now become part of the supply chain,” noted the report. “Cybersecurity risks in autonomous driving vehicles can have a direct impact on the safety of passengers, pedestrians, other vehicles and related infrastructures. It is therefore essential to investigate potential vulnerabilities introduced by the usage of AI.”

Researchers stressed the need for a strategy to determine how responsibility for damages and losses following a mass hacking of driverless cars would be determined. They suggested that a national body with a guaranteed fund to compensate victims might be the best solution for everyone involved.

“If manufacturers are required to pick up the burden of compensating victims of mass hacking, major disruptions to innovation would be likely. Disputes could result in litigation costs for both manufacturer and insurer,” observed Channon. “Public confidence requires a system to be available in the event of hacking or mass hacking which compensates people and also does not stifle or limit continuing development and innovation.”

To learn more about the potential benefits of self-driving cars, read "Driving Mr. and Ms. Daisy."
