Government action needed to ensure insurance against major hacking of driverless vehicles, experts warn

November 3 2021

The finalized prototype of Google self-driving car. Credit: Google

Government action is needed so driverless vehicles can be insured against malicious hacks which could have potentially catastrophic consequences, a study says.

The software in driverless vehicles will make it possible for them to

communicate with each other. It is being used and tested on public transport around the world, and is likely to be available to private vehicles in the future.

This technology can help improve transport safety, but hacking could result in accidents and damage to fleets of vehicles, financial loss, deaths and personal injury.

Experts have called for the creation of a national compensatory body in the UK offering a guarantee fund from which victims may seek redress.

Traditional vehicle insurance wouldn't cover the mass hacking of driverless cars, and an incident like this could cost the industry tens of billions of pounds.

Hackers could target vehicles via their regular software updates. Without appropriate insurance systems driverless vehicles could pose too great a danger to road users if the vehicles suffered serious software defects or were subject to malicious hacking. Existing systems of liability are deficient or inapplicable to vehicles which operate without a driver in control.

The research, published in the journal *Computer Law & Security Review*, was carried out by Matthew Channon from the University of Exeter and James Marson from Sheffield Hallam University.

Dr. Channon said that "it's impossible to measure the risk of driverless vehicles being hacked, but it's important to be prepared. 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 UK."

"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."

"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."

Dr. Marson concluded that "the UK intends to play a leading role in the development and roll-out of connected and autonomous vehicles. It was the first country to establish a statutory liability framework for the introduction of autonomous vehicles onto national roads. If it wishes to continue playing a leading role in this sector, it has the opportunity by creating an insurance fund for victims of mass-hacked vehicles. This would not only protect road users and pedestrians in the event of injury following a hacking event, but would also give confidence to insurers to provide cover for a new and largely untested market."

More information: Matthew Channon et al, The liability for cybersecurity breaches of connected and autonomous vehicles, *Computer Law & Security Review* (2021). DOI: 10.1016/j.clsr.2021.105628

Provided by University of Exeter