How to keep automated electric vehicles safe

28 April 2021, by Scott Michaux

Credit: Unsplash/CC0 Public Domain

Having your social media account hacked is a pain. Having your credit card account hacked can be devastating. Having your new electric vehicle hacked could be disastrous.

As the move toward automated electric cars accelerates, protecting the cybersecurity of these vehicles has become urgent. That's why University of Georgia researchers are identifying weaknesses that could threaten the safety and efficiency of such vehicles. In a new paper published in the *IEEE Journal of Emerging and Selected Topics in Power Electronics*, a UGA-led team provides the first comprehensive study on cyber-physical security of powertrain systems in connected and automated electric vehicles, or CAEVs.

"The results here will provide guidelines for manufacturers to develop better technologies against cyberattacks," said lead author Jin Ye, assistant professor of electrical engineering and director of the Intelligent Power Electronics and Electric Machines Laboratory. "As they design better and more secure vehicles, the manufacturers should take those aspects into consideration."

Safety concerns have long been at the forefront during the emergence of CAEVs. A recent fatal crash in Texas has only heightened those concerns.

For this study, the researchers investigated vulnerabilities to cyberattacks directed at targets ranging from energy efficiency to safety, and provided an architecture for next-generation power electronics systems.

Security studies of internal combustion engine vehicles don't address powertrain systems in CAEVs, which consist of multiple complex and integrated cyber-physical systems that require monitoring and control to guarantee safety and maintain high efficiency, according to Ye. In addition, increasing connectivity between CAEVs, charging stations and smart grids exposes CAEVs to cyberthreats that don't exist for internal combustion engines.

While technology such as adaptive cruise control and other auto-assist functions can significantly enhance driving safety, comfort and energy efficiency, embedding such control units into networked infrastructure opens a door to cybersecurity concerns. In-vehicle infotainment systems—used to deliver entertainment and useful information to the driver and the passengers through audio/video interfaces, touch-screen displays, button panels and voice commands—are a prime target for attackers, allowing them to hijack both safety-critical and non-safety functions.

Likewise, because electric vehicles plug into the grid to charge batteries, they are more vulnerable to cyberattack than conventional internal combustion engine vehicles. Through a charging station, an attacker could circumvent the vehicle control systems, which could lead to life-threatening consequences such as disabling brakes, turning off

headlights or taking over steering.

"Electric vehicles will be connected to many different infrastructures, so those connections will create cyberattack problems as well," Ye said.

Cyberattacks can also significantly reduce efficiency of electric vehicles, causing faster deterioration in power capability and battery life, thus shortening the time and distance between charging. Highly skilled attackers can potentially cause severe damage, such as decreasing battery capacity and energy by up to 50 percent, using sophisticated methods hardly detectable by the human driver.

"If a cyberattack happens, you will see some bad signals: Speed and acceleration of vehicles will be damaged, creating safety and functionality problems," Ye said. "Or it might create some problems in energy management systems. The efficiency of electric vehicles will go down, and the batteries are likely to die in a very short time. All the signals we studied will have negative impacts on safety."

Safety guidance for electric vehicles

Ye has written a series of articles on cyber-physical security in electric vehicles for the Institute of Electrical and Electronics Engineers, with two already published in April and May *IEEE Transactions* journals. Her emerging studies can enable carmakers and engineers to develop a first-stage cyber-security system. She suggests some basic mitigation techniques to defend modern vehicles against cyber-attacks:

- Secure on-board diagnostics port
- Better firewall
- Reliable hardware
- Secure software updates
- Penetration testing
- Code reviews

Most importantly, Ye suggests developing a cyber-security monitoring system to detect, locate, diagnose and mitigate cyberattacks.

"Even though the research of vehicle cyber-security is still at an early stage, and the monitoring system cannot directly recover the system to a safety region, it can alert the driver to react in a timely fashion," Ye said. "Once a cyberattack is identified, the driver can stop the car to avoid further damage."

More information: Jin Ye et al. Cyber-Physical Security of Powertrain Systems in Modern Electric Vehicles: Vulnerabilities, Challenges and Future Visions, *IEEE Journal of Emerging and Selected Topics in Power Electronics* (2020). DOI: 10.1109/JESTPE.2020.3045667

Provided by University of Georgia

APA citation: How to keep automated electric vehicles safe (2021, April 28) retrieved 9 December 2021 from https://techxplore.com/news/2021-04-automated-electric-vehicles-safe.html