Protecting your self-driving car, and your privacy, from cyberhackers in the age of AI

August 8 2023, by David Drucker

Credit: Unsplash/CC0 Public Domain

Imagine driving down the highway when suddenly your brakes slam, your engine turns off and your doors lock. A hacker has remotely taken control of your car.

Preventing this hypothetical scenario is a focus of automakers everywhere. As cars become loaded with computerized parts, they also become vulnerable to cyberattacks and privacy leaks, at least to a degree.

Professional "good guy" hackers demonstrated that they can attack computerized technology in cars as recently as this spring, when French security business Synacktiv proved that it could hack the infotainment system of a leading electric vehicle at the annual Pwn2Own computer hacking competition.

This cybersecurity sector is becoming more of a focal point for research, particularly as advancements in artificial intelligence (AI) make their way into the auto industry.

"If you have a classic car with almost zero computers, then there is almost no chance someone can remotely take control of your car. But now, with advancement and widespread integration of computing devices in modern cars, we are thinking about things differently," said M. Hadi Amini, an assistant professor at the Knight Foundation School of Computing and Information Sciences at FIU's College of Engineering and Computing.

Amini is an expert in developing machine learning, AI and optimization algorithms and tailoring them towards real world applications, including health care, homeland security and infrastructure resilience. He researches how to integrate AI into complex systems while considering cyber, physical and societal perspectives at the Sustainability, Optimization, and Learning for InterDependent networks laboratory (solid lab).

Amini is leading the university's investigation of AI for the National Center for Transportation Cybersecurity and Resiliency, which is funded by the U.S. Department of Transportation.

The potential of AI in vehicles is seemingly great—already, some drivers are using the technology to operate their vehicles semi-autonomously—but the technology also brings new challenges.

One of the key focuses is the storage of drivers' information. AI needs your data to make smarter decisions. So, Amini is looking into whether or not someone's personal information might be vulnerable if a car is hacked.

According to the Federal Trade Commission, a car's electronic system might store:

- Phone contacts
- Mobile app log-in information
- Location data
- Garage door codes

So a major cybersecurity concern for the auto industry arises. If the central server of a network of cars gets hacked, would that mean every driver's personal information in that network is up for grabs?

"Privacy is the first of many challenges we will face in applying classic AI algorithms to vehicles," Amini said. "Drivers of autonomous vehicles will want to use AI to help their cars perform better. The question is, how will drivers ensure that their data stays private while automakers use that data to improve vehicle performance?"

"If we are able to implement AI in a responsible, privacy-preserving and secure way, then we might be able to have more control over these

attacks."

The algorithms that power artificial intelligence are hungry for data, Amini explained. They become good at what they do by having a lot of examples to learn from.

But all this learning must take place somewhere. It needs to be computed. This often happens at a centralized, high-powered server.

Amini is exploring a way to use AI without having to ask all the drivers in a network to share their data to a central location. He is researching a more decentralized form of AI which would not rely as much on one central server. Instead, many of the computing and learning responsibilities would be left up to individual cars. Cars would digest data on their own and come up with suggestions to improve their algorithms.

These suggestions, which would not contain raw data, would then transmitted to servers that help improve the overall algorithm for all the devices in a network. The result: an AI network that is more difficult to steal personal information from.

Amini has been studying this form of AI and computing algorithms like it for about a decade. Today, this type of AI is best known as federated learning, a name that Google coined in 2016.

This style of AI has the potential to not only protect drivers' privacy, but also enable more efficient and scalable computing with an increasing number of cars, Amini said.

"In centralized machine learning, if we lose the power to the central server during an attack or a natural disaster, then the entire system will fail. But when we are operating in distributed machine learning, the rest

of the system can operate and continue functioning for some time by relying on local data," Amini said.

While no computerized system is ever 100% secure, Amini added, the research into federated learning provides a promising pathway for automakers to capitalize on advances in AI while protecting the personal information of drivers and ensuring the secure operation of transportation systems against cyberattacks.

Provided by Florida International University

Citation: Protecting your self-driving car, and your privacy, from cyberhackers in the age of AI (2023, August 8) retrieved 27 April 2024 from https://techxplore.com/news/2023-08-self-driving-car-privacy-cyberhackers-age.html