Technical Potholes for Autonomous Vehicles

With the future of autonomous vehicles moving closer, not only will engineers need to ensure defensive driving technology is up to scratch, they will have to design systems that defend vehicles against hackers whose purpose is to see them crash and burn.

Long haul trucks and metro taxis are the first vehicles on the list to go autonomous and while this might take the drudgery out of mundane driving, it will also take the jobs of those who drove them. And it's just around the corner. Ford has announced it is working with US ride-hail service Lyft to deploy self-driving cars on its platform by 2021. Engineers from both companies are collaborating on software to allow Fords to communicate with Lyft's app.

Widespread disenfranchisement of Uber, taxi, bus and truck drivers, together with teenagers and university graduates unable to get jobs, will make for fertile ground for would-be hackers. A Goldman Sachs report from May this year, estimated 300,000 US drivers would lose their jobs each year and that semi- and fully-autonomous car sales will have 20% market share by 2025-2030.

While car hacking is not a major issue yet, hackers will upskill as the technology in autonomous vehicles becomes more common. But researchers have already demonstrated remote control of a car's stereo and windshield wipers, as well as the engine and brakes. And hackers have already been able to disable and steal cars using their on-board computers.

Last year, researchers from the University of South Carolina, China's Zhejiang University, and Chinese security company Qihoo 360 demonstrated that sensors on a Tesla S could be jammed, making objects invisible to its navigation system as well as creating the perception of an object where there was none. The team used off-the-shelf radio-, sound- and light-emitting tools to deceive Tesla's autopilot sensors, with varying degrees of success.

When the big automakers declare car hacking is a safety issue, you know it's serious business. In July 2016, General Motors CEO Mary Barra said hacking would become a public safety issue that all manufacturers needed to work on together.

"The threat landscape is continually evolving, and sophisticated attacks are specifically designed to circumvent even the most robust defence systems," Barra said. She revealed that phishing, spyware, malware and ransomware attacks were getting "more and more sophisticated" so ITEE engineers certainly have their work cut out for them.

Return to the ITEE College Webpage