Team develops system to legally test GPS spoofing vulnerabilities in automated vehicles

30 April 2019

Credit: CC0 Public Domain

Southwest Research Institute has developed a cyber security system to test for vulnerabilities in automated vehicles and other technologies that use GPS receivers for positioning, navigation and timing.

"This is a legal way for us to improve the cyber resilience of autonomous vehicles by demonstrating a transmission of spoofed or manipulated GPS signals to allow for analysis of system responses," said Victor Murray, head of SwRI's Cyber Physical Systems Group in the Intelligent Systems Division.

GPS spoofing is a malicious attack that broadcasts incorrect signals to deceive GPS receivers, while GPS manipulation modifies a real GPS signal. GPS satellites orbiting the Earth pinpoint physical locations of GPS receivers embedded in everything from smartphones to ground vehicles and aircraft. SwRI designed the new tool to meet United States federal regulations. Testing for GPS vulnerabilities in a mobile environment had previously been difficult because federal law prohibits over-the-air re-transmission of GPS signals without prior authorization.

SwRI's spoofing test system places a physical component on or in line with a vehicle's GPS antenna and a ground station that remotely controls the GPS signal. The system receives the actual GPS signal from an on-vehicle antenna, processes it and inserts a spoofed signal, and then broadcasts the spoofed signal to the GPS receiver on the vehicle. This gives the spoofing system full control over a GPS receiver.

While testing the system on an automated vehicle on a test track, engineers were able to alter the vehicle's course by 10 meters, effectively causing it to drive off the road. The vehicle could also be forced to turn early or late.

"Most automated vehicles will not rely solely on GPS because they use a combination of sensors such as lidar, camera machine vision, GPS and other tools," Murray said. "However, GPS is a basis for positioning in a lot of systems, so it is important for manufacturers to have the ability to design technology to address vulnerabilities."

SwRI develops automotive cybersecurity solutions on embedded systems and internet of things (IoT) technology featuring networks and sensors. Connected and autonomous vehicles are vulnerable to cyber threats because they broadcast and receive signals for navigation and positioning.

The new system was developed through SwRI's internal research program. Future related research will explore the role of GPS spoofing in drones and aircraft.

Murray will present a poster on the system at AUVSI XPONENTIAL in Chicago on April 30 at Booth No. 3216 in XPO Hall. Visit SwRI's larger XPONENTIAL exhibit at Booth No. 1807 in the main hall.

For more information, visit https://www.swri.org/cyber-physical-systems-security or https://automateddriving.swri.org.

Provided by Southwest Research Institute