PRO CYBER COMMENTARY & ANALYSIS

How to Defend Against GPS Spoofing Attacks

By Adam Janofsky
Sept. 18, 2018 5:34 p.m. ET

As ship and car makers race to roll-out self-driving technology, security researchers warn that attacks using fake GPS signals could increase and become more dangerous.

U.S. government agencies including the National Science Foundation and the Department of Homeland Security have elevated the issue over the past year, issuing grants and guidance to address what's known as GPS spoofing.

GPS, or the Global Positioning System, was developed by the U.S. government for military navigation, but is accessible to anyone with a GPS receiver. These devices retrieve information from about 30 Department of Defense satellites, and that data is used to calculate the device's geographic location in real time.

GPS spoofing tricks these devices into collecting fake GPS signals, which leads them to calculate incorrect locations or travel times, according to Lee Neubecker, an independent cybersecurity researcher who has written about such attacks.

"Many cargo ships are increasingly dependent on GPS for navigation and steering," said Mr. Neubecker, who founded computer forensics firm Forensicon Inc. and sold it in 2016 to electronic-discovery firm **QDiscovery LLC**.

"With spoofing, you can't rely on a computer to solely control a ship or vehicle," he advised. "You need other systems to set off alarms and alerts that aren't so computer-dependent."

Steering Vehicles into Danger

The NSF issued grants this year to researchers working on ways to understand and prevent spoofing attacks. One paper funded by the NSF and published in July by researchers at Virginia Tech, Microsoft Research and the University of Electronic Science and Technology of China, demonstrated how hackers could use such an attack to steer an automobile to the wrong destination -- or into danger.

"The problem is critical considering that navigation systems are actively used by billions of drivers on the road and play a key role in autonomous vehicles," the researchers wrote.

The team used a $223 portable spoofing device to feed a car's navigation system with what they called a "ghost route." When tested on 40 drivers in the U.S. and China, 95% followed the navigation to the wrong destination without noticing the directions were wrong.

Real-world spoofing attacks have been reported but are difficult to corroborate. In 2017, the captain of a ship travelling to the Russian port of Novorossiysk noticed that his navigation system displayed its location about 30 miles away, at an airport, Wired reported. In June and December 2017, the Maritime Administration with the U.S. Department of Transportation warned of GPS interference reported in the Black Sea. "GPS disruptions are a global concern," a Maritime Administration bulletin said.

Researchers also have demonstrated how GPS spoofing might interfere with self-driving cars. However, these vehicles use a number of additional tools, such as pulsed laser light, to obtain a more detailed view of their surroundings than using GPS alone.

Guidance published by the Department of Homeland Security in 2017 recommends a number of measures that can help organizations avoid GPS spoofing and related attacks. Safeguards include obscuring antennas or installing decoy antennas to throw off attackers, adding sensors that can detect spoofing signals and send alerts to remote monitoring sites, and installing several antennas in different locations, which allow personnel to monitor for GPS discrepancies and other indicators of an attack.

DHS also called on GPS device manufacturers to implement anti-spoofing technology that recognizes, rejects and reports spoofing signals. "Upon

recognition and reporting of spoofing signals, the unit should hand over to a backup sensor [such as a] precision clock [or] inertial sensors," DHS said.

Rockwell Collins Inc., a manufacturer of military navigation satellite systems, said it uses Selective Availability Anti-Spoofing Module-based GPS receivers. This technology uses encryption to verify that GPS signals come from legitimate sources.