Legal Over-the-Air Spoofing of GPS and the Resulting Effects on Autonomous Vehicles

INTRODUCTION/BACKGROUND

Many systems rely on an accurate global positioning system (GPS) signal for normal operation. This is particularly true for autonomous vehicles and commercial and military aircraft. GPS is preferred because the positional errors are not related to the location of the receiver and the position is computed relative to a globally defined coordinate system.

However, GPS is vulnerable to external interference. In commercial applications, it is common for GPS to be blocked, distorted, or reflected by buildings, tunnels, overpasses, or other structures. It is highly desirable to be able to test the vulnerability of GPS receivers and their system's response to interference in a natural, controlled environment.

Testing is difficult because U.S. federal law prohibits over-the-air retransmission of GPS signals without appropriate authority.

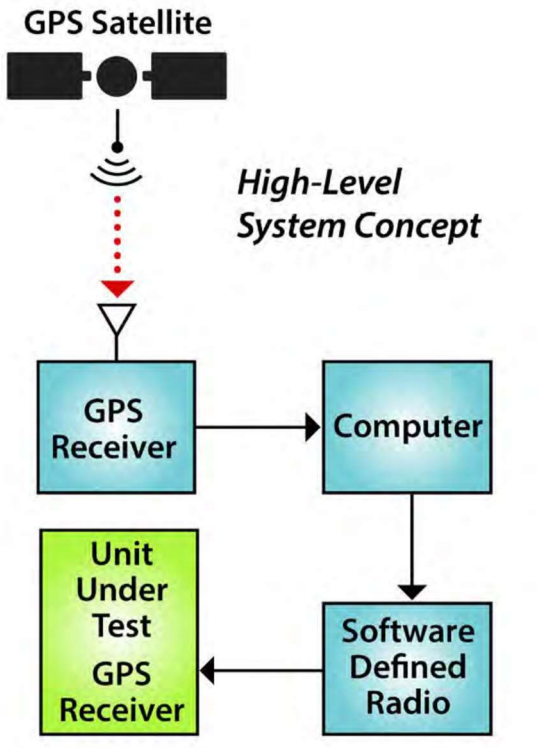
So, what is allowed?

In general, the Federal Communications Commission (FCC) authorizes entities to reradiate GPS signals and on other restricted frequencies under three scenarios:

1. inside a fully enclosed Faraday cage
2. under an experimental license (47 C.F.R. §5.53)
3. under a waiver of the FCC's rules (47 C.F.R. §1.3).

This research, performed and funded by Southwest Research Institute® (SwRI®), demonstrated the usefulness of a mobile GPS spoofing system, which will enable legal, real-world evaluation of GPS vulnerabilities. The system has two physically separate pieces:

- an on-vehicle box that is placed on top of the vehicle's GPS antenna
- a ground station that controls the attacks remotely



The system receives the actual GPS signal from an on-vehicle antenna, processes it, inserts a spoofed signal, and broadcasts the spoofed signal to the vehicle's GPS receiver, as shown at right. This gives the spoofing system full control over the vehicle's GPS receiver and allows for real-time manipulation while a receiver is in motion.

The operator can modify the signal remotely in real time through the graphical user interface (GUI).

EFFECTS ON AUTONOMOUS VEHICLES

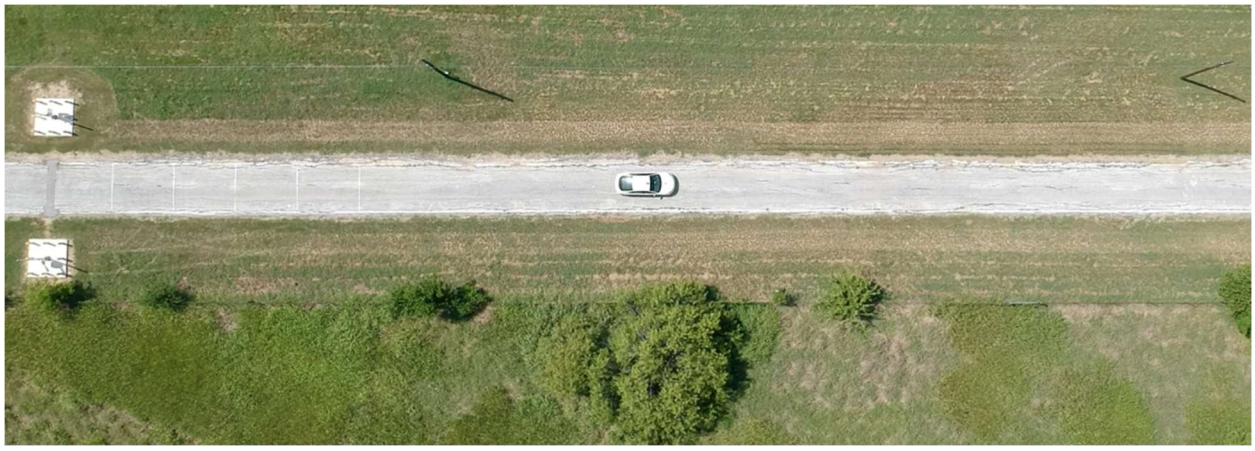
Offset Insertions

A user can insert an offset in any direction and by any distance to manipulate the perceived location of the vehicle under test.

Results

Vehicle location could be translated up to about ten meters at a time. Shifting left or right, the vehicle would immediately compensate and move in the opposite direction. This provided the ability to force lane changes, drive the car off the road, or cause it to turn early or late if an offset was applied to the direction of travel.

Altered GPS



Normal

Velocity Attacks

The GPS speed was intentionally varied, and the effects were observed.

Results

- When implemented during a turn, the vehicle would turn too far and run off the road.
- When implemented before a turn, the vehicle would turn early or late.
- When performed on a straight section, the vehicle did not change speed and would continue on the same route.

Altered GPS

Normal

Halt

The GPS speed was slowly brought to a halt.

Results

- While GPS speed was reduced, the vehicle continued to drive at the same speed. When the GPS location was static, the vehicle's control system became unstable due to lack of accurate positional feedback.
- When broadcasting the final coordinate in the waypoint list or the end of the planned path to the vehicle, it would come to a stop believing that it had completed the route.

Altered GPS

Normal

Timing Attacks

The actual vehicle position was replayed to the GPS receiver but delayed by several seconds.

Results

The vehicle steered randomly due to a lack of current positional feedback.

Jamming

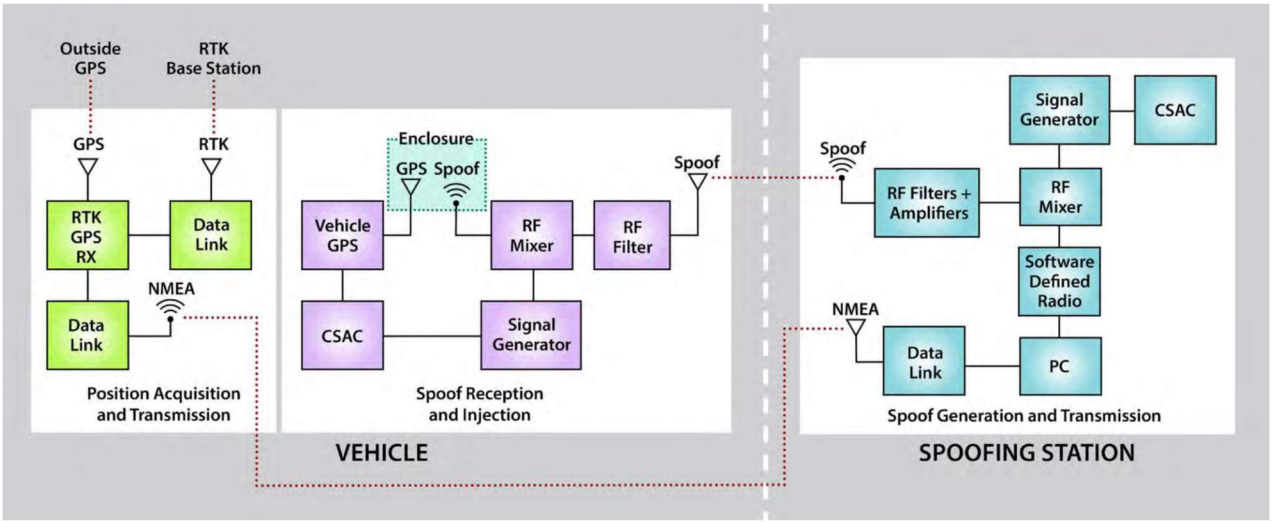
This is the simplest attack, since low-cost devices that can jam the GPS signal are available online for close to $30. Similar to the timing attacks, the vehicle steered randomly due to a lack of current positional feedback.

FREQUENCY TRANSLATION OF GPS SIGNALS

Most of the project used Wi-Fi or cellular links to remotely control the spoofing system. We also demonstrated frequency translation of GPS signals to an unlicensed band. To avoid over-the-air transmission of GPS signals, we used frequency translation to down-convert from the 1575.42MHz carrier to a 915MHz carrier in the ISM band. This is done by mixing the 1575.42MHz radio-frequency (RF) signal with a 660.42MHz signal from a local oscillator (LO), and then filtering and amplifying the combined signal.

On the receiver side, the signal is up-converted back to 1575.42MHz. This is done using a similar setup. Here, the LO frequency is kept at 660.42MHz, and the RF signal is at 915MHz. Then, we select the sum frequency at 1575.42MHz and reject the difference frequency at 254.58MHz.

The up-conversion and down-conversion process is shown below.



CONCLUSION

GPS plays a vital role in multiple facets of many modern-day systems. Due to the inherent vulnerabilities of GPS receivers, testing these vulnerabilities in systems is critical. U.S. federal law prohibits over-the-air spoofing which previously made testing these vulnerabilities outside of an enclosed laboratory environment difficult. SwRI demonstrated the ability to legally transmit a spoofed GPS signal on a mobile system to allow for analysis of the system responses.

NEXT STEPS

Testing described in this document is at a technology readiness level 5 (TRL-5), which means it is a developmental system that has been demonstrated in a relevant environment. Please contact us if you are interested in our GPS testing services or funding related research.

Victor C. Murray, CISSP®
Group Leader R&D
(210) 522-6589
victor.murray@swri.org

Additional information can be found on our websites:

https://www.swri.org/cyber-physical-systems-security

https://www.swri.org/automotive-cyber-security

https://www.swri.org/industry/sensing-perception-automotive-software-unmanned-systems-automotive-software-electronics