Untrustworthy Utility?

Ease with which GPS can be spoofed raises concerns about civil UAVs

Graham Warwick and Jen DiMascio Washington

A video of a small unmanned helicopter dropping from hover like a stone, its operator unaware control has been hijacked, threatens plans to open civil airspace to UAS (unmanned aerial systems) by exposing the vulnerability of GPS to counterfeit signals, or spoofing.

Although the weaknesses of civil GPS have implications beyond aviation—threatening the energy, financial and telecommunications sectors—they have come into sharp focus since Congress directed the FAA to open national airspace to UAS by 2015 (see p. 52).

Several lawmakers seemed to be having second thoughts during a July 18 hearing of a House homeland-security subcommittee, as University of Texas (UT) at Austin Assistant Prof. Todd Humphreys described tests that showed how vulnerable a civil UAS's GPS navigation system is to hacking.

For its demonstration, first in a football stadium and then for the Department of Homeland Security (DHS) at White Sands Missile Range, N.M., UT's Radionavigation Laboratory used Adaptive Flight's Hornet Mini, an $80,000 unmanned helicopter typical of UAS used by law enforcement.

At White Sands, the operator commanded the aircraft to hover at 50 ft., and a spoofer on a hilltop half a mile away began transmitting weak counterfeit GPS signals, "achieving meter-level alignment with the authentic signals at the location of the UAV's GPS antenna," says Humphreys.

"The spoofer then rapidly increased its counterfeit signal power, bringing the UAV under its control" by hijacking the GPS receiver's tracking loops. By inducing a false upward drift in the UAS's perceived location, the spoofer fooled the onboard flight controller into commanding a dive. The UAS "came straight down like an elevator in a shaft, entirely under control of the remote hacker." At about 10 ft. above the ground, a safety pilot took manual control.

The Hornet Mini is fairly sophisticated and representative of larger commercial UAS, with a navigation system built around a Kalman filter combining data from an altimeter, magnetometer and inertial measurement unit as well as a civil GPS with receiver autonomous integrity monitoring (RAIM) to identify and discard signals that appear to be outliers. "Standard RAIM is ineffective against GPS spoofing because it generates a fully self-consistent ensemble of spoofing signals; there are no outliers," says Humphreys.

Spoofing did not touch the aircraft's command-and-control or payload data links (which could be encrypted), only the unprotected civil GPS, and the UAS operator was unaware of the hijack. "The remote operator was in contact with the UAV the entire time, but nothing appeared wrong to his sensors."

UNIVERSITY OF TEXAS AT AUSTIN

UT's Humphreys, here with Hornet Mini UAV, brought media spotlight on GPS spoofing with a June demo in the university's football stadium.

Adaptive Flight CEO Wayne Pickell says the Hornet Mini has a "patent-pending GPS-denied operational mode" that was turned off for the UT demo, but adds that the company "is proud to be working with Dr. Humphreys and his team in their efforts to address GPS system vulnerabilities due to spoofing."

Sophisticated spoofers are not easy to build, but GPS simulators "can do almost everything that we did, and are readily available," says Humphreys. "So I am worried it could be a weapon in the arsenal of organized crime, state actors or terrorists."

"Spoofing is not a new issue," says Michael Toscano, CEO of the Association for Unmanned Vehicle Systems International (AUVSI). "[It] has implications for any technology that depends on GPS for guidance and timing, whether it is manned or unmanned aircraft, your cellphone or your car."

AUVSI believes military anti-spoofing technology will move into the civil market. Humphreys is doubtful, believing these so-called Saasm (selective availability anti-spoofing module) receivers would drive up the price of small UAS and create the logistical headache of distributing cryptographic keys while keeping them out of the wrong hands.

But Rockwell Collins argues its MicroGram miniature protected GPS is both tamper-proof and relatively inexpensive. "We think there is a technical solution," says Bobby Sturgell, vice president of Washington operations.

Despite his spoofing demo, Humphreys is "not terribly worried"—for now. Weighing only 13 lb., the UAS used would not cause much damage if hijacked and crashed. And it is not clear a hacker could do more. "It's not terribly easy to control it once you've got it," he says. "The question we have been asking ourselves is what actually could be done after you've captured it?"

But Humphreys' "nightmare scenario" is to look forward three or four years "to where we have adopted UAVs into national airspace without addressing this [vulnerability], and now the problem is scaling up so we have heavier UAVs. The FAA has predicted that, by 2020, there could be 30,000 of these flying in our airspace. That does concern me."

Humphreys is recommending that a spoof-resistant navigation system be required in UAS exceeding 18 lb. The U.S. Air Force is prepared to modify civil GPS signals with a cryptographic authentication signature, he says, but lacks the funds. "I believe it would fall to the DHS to fund something like this. I can't say I'm terribly optimistic."

A "grassroots" approach to building anti-spoofing into civil GPS may be more practical. "There are reasonable techniques you can bake into the GPS receivers and navigation systems of UAVs. While they won't prevent sophisticated attacks, they would make them much harder," he says. "The fact is, anti-spoofing is hard. There's no quick and easy and cheap solution, but there are cost-effective measures we can take in the short term."