'Spoofed' GPS signals can be countered, researchers show

July 24 2012, By Anne Ju

(Phys.org) -- From cars to commercial airplanes to military drones, global positioning system (GPS) technology is everywhere -- and Cornell researchers have known for years that it can be hacked, or as they call it, "spoofed." The best defense, they say, is to create countermeasures that unscrupulous GPS spoofers can't deceive.

Researchers led by Mark Psiaki, professor of mechanical and aerospace engineering, got to test their latest protections against GPS spoofing during a Department of Homeland Security-sponsored demonstration last month in the New Mexico desert at the White Sands Missile Range.

The much-publicized June 19 demo of a mini helicopter's GPS signal being spoofed was led by Todd Humphreys, Ph.D. '08, now an assistant professor at the University of Texas, Austin. Humphreys, who designed a sophisticated GPS spoofing system as an outgrowth of his Cornell Ph.D. and postdoctoral studies, also testified before Congress July 19 on the threat of GPS spoofing.

GPS is a navigation and timing system of satellites that circle Earth and transmit signals to receivers on land, sea and air to provide precise information on the receivers' locations and clock offsets. Lesser known is its ubiquitous presence in, for example, commercial and military aircraft navigation, control of the power grid, cell phone towers and even automated stock trades.

Spoofing is the transmission of false GPS signals that receivers accept as

authentic ones, theoretically allowing hackers to gain control over planes, vehicles or other devices that rely on GPS for navigation or timing.

On June 19, Humphreys and colleagues set out to demonstrate how a spoofing attack works, using live "on-air" transmissions, with permission from the Department of Homeland Security, to confuse real GPS signals in a remote area in New Mexico. Using fake GPS transmissions from about half a kilometer (0.3 miles) away, they hijacked a mini drone, causing it to dip violently because it assumed it was inadvertently climbing when, in reality, it had been hovering at its desired altitude.

On the sidelines were Cornell researchers Psiaki, senior engineer Steve Powell and graduate students Brady O'Hanlon and Ryan Mitch. They were testing a receiver modification that can differentiate spoofed GPS signals from real ones.

"The idea is not just for us to make spoofers so we can show bad things can happen, but also to gain insight into countermeasures in typical GPS receivers so they can be less vulnerable to attack," Powell said.

Psiaki said their latest countermeasure allowed the Cornell group to correctly detect spoofing in three cases during the demo. "This is strong confirmation that our system can successfully detect spoofing in an autonomous mode using short segments of GPS receiver data. It is the first known detection of this type of attack from a live, on-air spoofer," Psiaki said.

An earlier, less sophisticated spoofing detector developed at Cornell is patent pending. Data from this latest demonstration will form the basis of a scientific paper, and a decision to apply for patent protection is forthcoming, according to Psiaki.

GPS spoofing isn't exactly on the collective consciousness, but it is a

growing threat: Last year, Iran claimed to have spoofed -- and downed -- a GPS-guided American drone. Such an attack, Psiaki said, might have been carried out using techniques similar to those demonstrated at White Sands if the drone had been using civilian GPS signals. It is not unimaginable, he continued, that the Iranians (possibly with outside help) could have conducted a spoofing-like attack that used encrypted military GPS signals.

Psiaki also said that currently available GPS anti-spoofing technology, called Receiver Autonomous Integrity Monitoring, would not work with the smarter spoofers that Humphreys began developing in 2008 in collaboration with the Cornell GPS group.

"[Humphreys] has developed the baddest known spoofer there is," Psiaki said. "It's a great 'war games' tool that provides realistic attack scenarios for testing improved spoofing defenses. We're happy that our ongoing collaboration has produced several strong defenses that, taken together, may lay this national threat to rest."

Provided by Cornell University