

UT researchers show how easy it is to spoof unencrypted GPS signals used by drones

June 27 2012, by Bob Yirka



Armed Predator drone firing Hellfire missile. Image: Wikipedia.

(Phys.org) -- Professor Todd Humphreys of the University of Texas is making a lot of people nervous. First he and his team demonstrated their ability to circumvent the signals a drone flying over the university stadium was using to plot its course, causing it to nearly crash into the ground, before suddenly saving it from certain destruction. And as if that wasn't enough to make the point that drones flying using unencrypted GPS signals are vulnerable to spoofing, surely another demonstration he and his team gave for representatives of the Federal Aviation Administration and Department of Homeland Security drove the point home. They were very easily able to fool a drone in a test at White Sands Missile Range, with an inexpensively made device, into following the commands given by his team on multiple occasions.

Up till now, the main concern regarding drones, other than privacy or

moral issues, has been the knowledge that practically anyone can obtain a jamming [device](#) that prevents a drone from hearing GPS signals being sent by a satellite, thereby causing it to fly blind. Most such drones are programmed to land themselves if such an event occurs. Many believe this is exactly what happened last year when Iran claimed to have successfully brought down a US military drone flying over its airspace. Unfortunately, it appears, there is a far greater threat and it comes from spoofers, rather than jammers.

Spoofers are devices that fool other devices into believing that it's the device they are supposed to be communicating with. In the case of drones, a spoofing device can send out a signal that is stronger than the signal the drone receives from a satellite. By matching the signal, the spoofer is able to fool the drone into thinking it's still getting its data from the satellite and thus becomes a trusted source. Once that occurs, those running the spoofing device can send commands to the drone causing it to behave as they indicate, ignoring those that come from other sources, in essence, allowing the drone to be hijacked by anyone with such a device. It should be noted that this is only possible with drones that use *unencrypted* GPS signaling, e.g. most non-military drones.

Humphreys told the officials at the demo that all of his equipment together cost only about a thousand dollars to put together, meaning the technology is easily accessible by anyone wishing to take over a [drone](#) for purposes other than for demonstration. In such cases, drones could be made to crash into buildings, sporting stadiums, other planes or any other target they choose. Particularly troubling is the fact that the FAA has outlined a plan for allowing commercial drones to fly in the United States by 2015, most of which would be flying using unencrypted GPS signals.

Humphreys and his team are hoping the demonstrations convince

government officials to make changes to requirements on [GPS](#) signaling devices on drones before allowing them to fly in US air space.

More information: radionavlab.ae.utexas.edu/

via [Fox](#)

© 2012 Phys.Org

Citation: UT researchers show how easy it is to spoof unencrypted GPS signals used by drones (2012, June 27) retrieved 19 April 2024 from <https://phys.org/news/2012-06-ut-easy-spoof-unencrypted-gps.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--