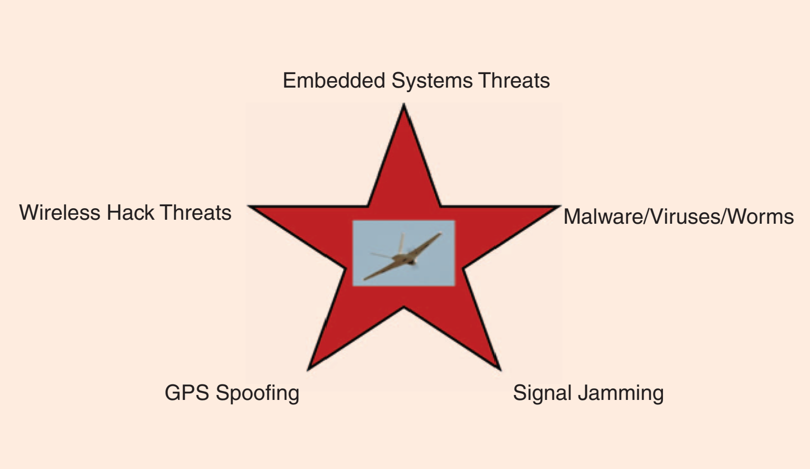
Donna A. Dulo

Unmanned Aircraft: The Rising Risk of Hostile Takeover

The use of unmanned aircraft also known as drones is increasing in U.S. national airspace and the numbers will rise exponentially once the Federal Aviation Administration (FAA) formally opens up the skies to drones in the next few years. The result will be the addition of tens of thousands of unmanned aircraft in the sky, in addition to the ever increasing manned aircraft traffic, resulting in significant safety concerns.

A threat to safety that is commonly overlooked when operating an unmanned aircraft is the threat of a hostile takeover. A hostile third party can wreak havoc in the skies with a malicious drone traversing the airspace with ominous intentions. Whether of portentous terrorist origins or merely a young experimenter testing their technical prowess, a third party controlled drone can work its way into the intake of a jetliner potentially bringing it down, or negotiate its way across the skies, ultimately crashing on innocent bystanders. The range of potential damage and human injury is considerable. Unfortunately, the information assurance and security aspects of unmanned aircraft have taken a back seat to privacy and myriad safety concerns. Yet information assurance and security in drones is a safety as well as privacy threat, since a hostile unmanned aircraft can be hard to trace, track, and ultimately control.



A System of Systems Aerial Target

An unmanned aircraft is, in engineering terms a "system of systems." This means that it is a combination of various inherently complex systems, all operating in tandem to perform a given aerial task. From the aircraft itself to the ground station as well as GPS satellites and communication networks, the unmanned aircraft system is a highly complex computationally and electronically based structure, manifesting the same vulnerabilities as other computational and electronic network based systems as well as presenting unique vulnerabilities that are ripe for exploitation from dangerous emerging threats. In addition, being a system of systems, the unmanned aircraft system is at risk from multiple or

Digital Object Identifier 10.1109/MTS.2015.2461196
Date of publication: 16 September 2015

blended threats, which may attack various systems at once making the defense of the aircraft both multifarious and technically dynamic as threats continually evolve.

The threat of hostile takeover is a multi-dimensional threat that can emerge in many ways through the unmanned aircraft system of systems. A spectrum of attacks can manifest through communicational and computational channels in both the aircraft itself as well as the ground control station through software, hardware, embedded systems, network components, and other control structures. In many ways, an unmanned aircraft can be considered as a wireless device/node in the sky, open to the same threats as a wireless network. It is also open to attacks through communication and GPS signals. In a broad sense, five distinct threat domains can be discerned in a hostile takeover threat spectrum: embedded system threats, malicious software threats (malware), wireless hack threats, GPS spoofing, and signal jamming. Each can be considered as a formidable menace to unmanned aircraft security, with a blending of these threats being a latent prospect as aerial operations become ubiquitous in the national airspace.

> Hostile takeover threats to unmanned aerial systems are real and imminent.

Embedded Systems Threats

Embedded systems security is a major concern for the unmanned aerial system. Embedded systems tend to have generic hardware and software which in many cases come from foreign countries that do not have mandatory development process security protocols. This can result in built-in vulnerabilities and malicious logic errors in the integrated circuits as well as the software that drives the chips. The interconnectivity of the various embedded systems makes these logic vulnerabilities pervasive throughout the system.

Embedded components such as integrated circuits, programmable logic controllers, and industrial control-type mechanisms can inflict physical as well as informational damage in both the aircraft and the ground control station. Controllers that operate in real time have the potential to manipulate electrical outputs based on the logic structures of the circuit. If a malicious logic structure manifests in real time, the devices connected to the controller such as sensors, aerial control structures, motors, or other electromotive devices can be malevolently manipulated. Thus through adverse computational logic, erroneous electrical impulses in the hardware can result in malicious control or a catastrophic failure of the aircraft in real time.

Malicious Software Threats

Malicious software threats can emerge in an unmanned aerial system through any one of the computational systems in both the aircraft and the ground control system. These threats are similar to most computational systems: viruses, worms, spyware, as well as innumerable forms of malware. Malicious software can result in hostile aircraft control through many channels such as network based intrusion, software exploitation, communication signal manipulation, as well as flight control hijacking. The possibilities of nefarious malware manipulation are virtually endless. The plethora of malware mechanisms make their manipulation a formidable threat to unmanned aircraft.

Wireless Hack Threats

Drones are unmanned aircraft on a wireless tether when they are not autonomously flown. This means that they are open to traditional wireless network hacks and exploits resulting in a hostile takeover of the aircraft. Threats include packet injection, re-authentication, and script code injection, as well as other threats to the wireless network components within the system of systems. Wireless hacks can be directed at the aircraft, the ground station or both.

GPS Spoofing Threats

GPS civilian signals are founded upon an open standard with free accessibility signals, no form of authentication, all on top of unencrypted signals. The transparency and predictability of GPS signals have created an inherent weakness in the system: the ability for GPS signals to be spoofed, which means the signals can be maliciously replicated with ease. An unmanned aircraft can be hijacked, controlled and ultimately crashed by spoofing its live, real-time GPS signals. GPS spoofing can occur in many ways such as through live satellite signal spoofing, software code spoofing as well as differential corrections spoofing. Regardless of the mechanism, GPS spoofing poses a critical danger to unmanned aircraft as the open nature of civilian GPS creates a wide range of technical spoofs that are relatively easy to formulate and implement.

Signal Jamming Threats

Signal jamming is a major issue with the cyber-physical aspects of unmanned aircraft. Signal jamming can be a single or multi-path endeavor affecting many of the aircraft systems. Jamming signals can block GPS signals, communication signals, command and control signals, network signals, as well as signals from various aircraft systems such as anti-collision systems. The result is a weakened aircraft system that may face a loss of control, inaccurate navigation, or incomplete commands resulting in an unplanned traverse across the sky or a catastrophic event. Signal jamming is also dangerous as it opens up the aircraft system to other forms of exploits, compounding the ability to defend from the hostile threat.

Hostile Takeover Threats are Real and Imminent

The operation of unmanned aircraft in the skies has the potential to transform aviation. However the hostile takeover threats to these aerial systems are real and imminent. All operators must be cognizant to the hostile takeover threat and provide adequate countermeasures to these threats to not only protect the aircraft, but also to protect lives and property that are in the path of these innovative aerial machines. The time to take unmanned aerial security seriously is now.

Author Information

Donna A. Dulo, JD, is a mathematician, computer scientist, and systems engineer and has worked for the U.S. Department of Defense in military and civilian capacities for over 27 years. She is the President and Founder of the Unmanned Aircraft Safety and Security Society, Inc. dedicated to the safe and secure operation of unmanned aircraft in the national airspace. She is also a legal scholar and writer, and is the editor and lead author of the American Bar Association's book on unmanned aircraft law and technology, published in August of 2015.

> In many ways, an unmanned aircraft can be considered as a wireless device/node in the sky, open to the same threats as a wireless network.

OPINION *(continued from page 14)*

4) Set your devices not to broadcast their SSID. This step makes your devices less visible to the public (but admittedly won't slow down a dedicated hacker). The SSID is the device name that broadcasts, showing that a wireless connection to it is possible.

Note that implementing new security protections will make your camera less vulnerable, but there's still a chance it could be hijacked. A sophisticated hacker could not only violate your privacy by turning your webcam on you and your loved ones, but could also commandeer your network and make your camera a slave bot to carry out additional exploits.

The very best way to keep your IP camera from being turned on you is to not have it turned on in the first place. Use one if you must, but think very carefully about the potential damage that could be done when you click the "on" button.

Acknowledgement

This article has been adapted from Katherine Albrecht, Liz McIntyre, "Privacy Nightmare: When Baby Monitors Go Bad," Sept. 26, 2014; http://www.ehow.com/ehow-tech/blog/privacy-nightmare-when-baby-monitors-go-bad/.

References

[1] A. Wagner, "FOX19 Investigates: Hacker hijacks baby monitor," Apr. 25, 2014; http://www.fox19.com/story/25310628/hacked-baby-monitor.

[2] O.B. Waxman, "Stranger hacks into baby monitor and screams at child," Apr. 28, 2014; http://time.com/79170/stranger-hacks-into-baby-monitor-and-screams-at-child/

[3] S. Murphy and I. Gallagher, "How 'home hackers' spy on you and your children," Sept. 20, 2014; http://www.dailymail.co.uk/news/article-2763664/How-home-hackers-spy-children-YOUR-webcam-The-shocking-evidence-shows-private-lives-snooped-streamed-live-web.html#ixzz3LPZaihaT.

[4] K. Komando, Oct. 17, 2014; https://www.komando.com/tips/9092/dont-make-these-common-mistakes-with-your-passwords.