PHYS.ORG

Team makes hobby drones crash to expose design flaws

June 8 2016

Johns Hopkins computer science graduate students and their professor discovered three security flaws in a popular hobby drone, all of which could which cause the small aircraft to make an "uncontrolled landing." Credit: Will

Kirk/Johns Hopkins University

Sales of drones—small flying machines equipped with cameras—are soaring. But new research by a Johns Hopkins computer security team has raised concerns about how easily hackers could cause these robotic devices to ignore their human controllers and land or, more drastically, crash.

Five graduate students and their professor discovered three different ways to send rogue commands from a computer laptop to interfere with an airborne hobby drone's normal operation and land it or send it plummeting.

The finding is important because drones, also called unmanned aerial vehicles, have become so popular that they are, pardon the expression, flying off the shelves. A recent article in Fortune, referring to the 12-month period ending in April, trumpeted that Drone Sales Have Tripled in the Last Year. And the devices are not cheap. The article stated that the average cost of a drone was more than $550, though prices vary widely depending on the sophistication of the device. A recent Federal Aviation Administration report predicted that 2.5 million hobby-type and commercial drones would be sold in 2016.

Hobby drones are flown largely for recreation and aerial photography or videography. But more advanced commercial drones can handle more demanding tasks. Farmers have begun using drones with specialized cameras to survey their fields and help determine when and where water and fertilizer should be applied. Advanced commercial drones can also help in search and rescue missions located in challenging terrain. Some businesses, such as Amazon, are exploring the use of drones to deliver merchandise to their customers.

But in their haste to satisfy consumer demands, drone makers may have left a few digital doors unlocked. "You see it with a lot of new technology," said. Lanier A. Watkins, who supervised the recent drone research at Johns Hopkins' Homewood campus. "Security is often an afterthought. The value of our work is in showing that the technology in these drones is highly vulnerable to hackers."

Watkins is a senior cyber security research scientist in the university's Whiting School of Engineering, Department of Computer Science. He also holds appointments with the Johns Hopkins Applied Physics Laboratory and the Johns Hopkins Information Security Institute.

During the past school year, Watkins' master's degree students were required to apply what they'd learned about information security by completing a capstone project. Watkins suggested they do wireless network penetration testing on a popular hobby drone and develop "exploits" from the vulnerabilities found to disrupt the process that enables a drone's operator on the ground to manage its flight.

Lanier A. Watkins, left, a Johns Hopkins cybersecurity research scientist, worked with five graduate students, including Michael Hooper, at right, to determine that the technology used in a hobby drone was vulnerable to hacking. Credit: Will Kirk/Johns Hopkins University

An "exploit," explained Michael Hooper, one of the student researchers, "is a piece of software typically directed at a computer program or device to take advantage of a programming error or flaw in that device."

In the team's first successful exploit, the students bombarded a drone with about 1,000 wireless connection requests in rapid succession, each asking for control of the airborne device. This digital deluge overloaded the aircraft's central processing unit, causing it to shut down. That sent the drone into what the team referred to as "an uncontrolled landing."

In the second successful hack, the team sent the drone an exceptionally large data packet, exceeding the capacity of a buffer in the aircraft's flight application. Again, this caused the drone to crash.

For the third exploit, the researchers repeatedly sent a fake digital packet from their laptop to the drone's controller, telling it that the packet's sender was the drone itself. Eventually, the researchers said, the drone's controller started to "believe" that the packet sender was indeed the aircraft itself. It severed its own contact with the drone, which eventually led to the drone making an emergency landing.

"We found three points that were actually vulnerable, and they were vulnerable in a way that we could actually build exploits for," Watkins said. "We demonstrated here that not only could someone remotely force the drone to land, but they could also remotely crash it in their yard and just take it."

In accordance with university policy, the researchers described their drone exploit findings in a Vulnerability Disclosure Package and sent it early this year to the maker of the drone that was tested. By the end of May, the company had not responded to the findings. More recently, the researchers have begun testing higher-priced drone models to see if these devices are similarly vulnerable to hacking.

Watkins said he hopes the studies serve as a wake-up call so that future drones for recreation, aerial photography, package deliveries and other commercial and public safety tasks will leave the factories with enhanced security features already on board, instead of relying on later "bug fix" updates, when it may be too late.

Provided by Johns Hopkins University

Citation: Team makes hobby drones crash to expose design flaws (2016, June 8) retrieved 26 April 2024 from https://phys.org/news/2016-06-team-hobby-drones-expose-flaws.html