Wireless devices used by casual pilots vulnerable to hacking, computer scientists find

November 10 2014

Computer science Ph.D. student Devin Lundberg holds the three devices the researchers examined. From left: the Appareo Stratus 2, the SageTech Clarity CL01 and the Garmin GDL 39. Credit: Jacobs School of Engineering/UC San Diego

A new class of apps and wireless devices used by private pilots during flights for everything from GPS information to data about nearby aircraft is vulnerable to a wide range of security attacks, which in some scenarios could lead to catastrophic outcomes, according to computer scientists at the University of California, San Diego and Johns Hopkins University. They presented their findings Nov. 5 at the 21st ACM Conference on Computer and Communications Security in Scottsdale, Ariz.

Researchers examined three combinations of devices and apps most commonly used by private pilots: the Appareo Stratus 2 receiver with the ForeFlight app; the Garmin GDL 39 receiver with the Garmin Pilot app; and the SageTech Clarity CL01 with the WingX Pro7 app. The devices and apps allow casual pilots to access the same information available to the pilot of a private jet—at a fraction of the cost. All the instruments in a high-end cockpit can be valued at more than $20,000. By contrast, the systems the researchers examined are available for $1,000. All have to be paired with tablet computers, most often an iPad, to display information.

The devices researchers examined receive information about the aircraft 's location, the weather, the location of nearby aircraft the and airspace restrictions, which they display on the tablet computers via an app. "When you attack these devices, you don't have control over the aircraft, but you have control over the information the pilot sees," said Kirill Levchenko, a computer scientist at the Jacobs School of Engineering at UC San Diego, who led the study.

ForeFlight, which pairs with the Appareo Stratus 2, is one of the top 50 grossing apps in the entire Apple App Store—ahead of Apple's own Pages app, among others.

The team hoped that exposing the systems' vulnerabilities would increase

awareness among users and lead to demands for change. Researchers include several recommendations at the end of their study for safety improvements.

The FAA has the authority to regulate these systems but chooses not to because they are not an integral part of the aircraft, the researchers said. In commercial aircraft the FAA only allows static information, such as maps, to be displayed on tablet computers, cautioning pilots to rely on instruments to fly.

During testing, researchers found significant safety flaws in all three systems. Two of the systems allowed an attacker to replace completely the firmware, which is home to the programs controlling the devices. The Appareo Stratus 2 allowed the firmware to be downgraded to any older version. All three devices allowed an attacker to tamper with the communication between receiver and tablet. Both types of attacks give an attacker full control over safety-critical real-time information shown to the pilot.

The devices are paired with iPad apps, which also had some vulnerabilities. Credit: Jacobs School of Engineering/UC San Diego

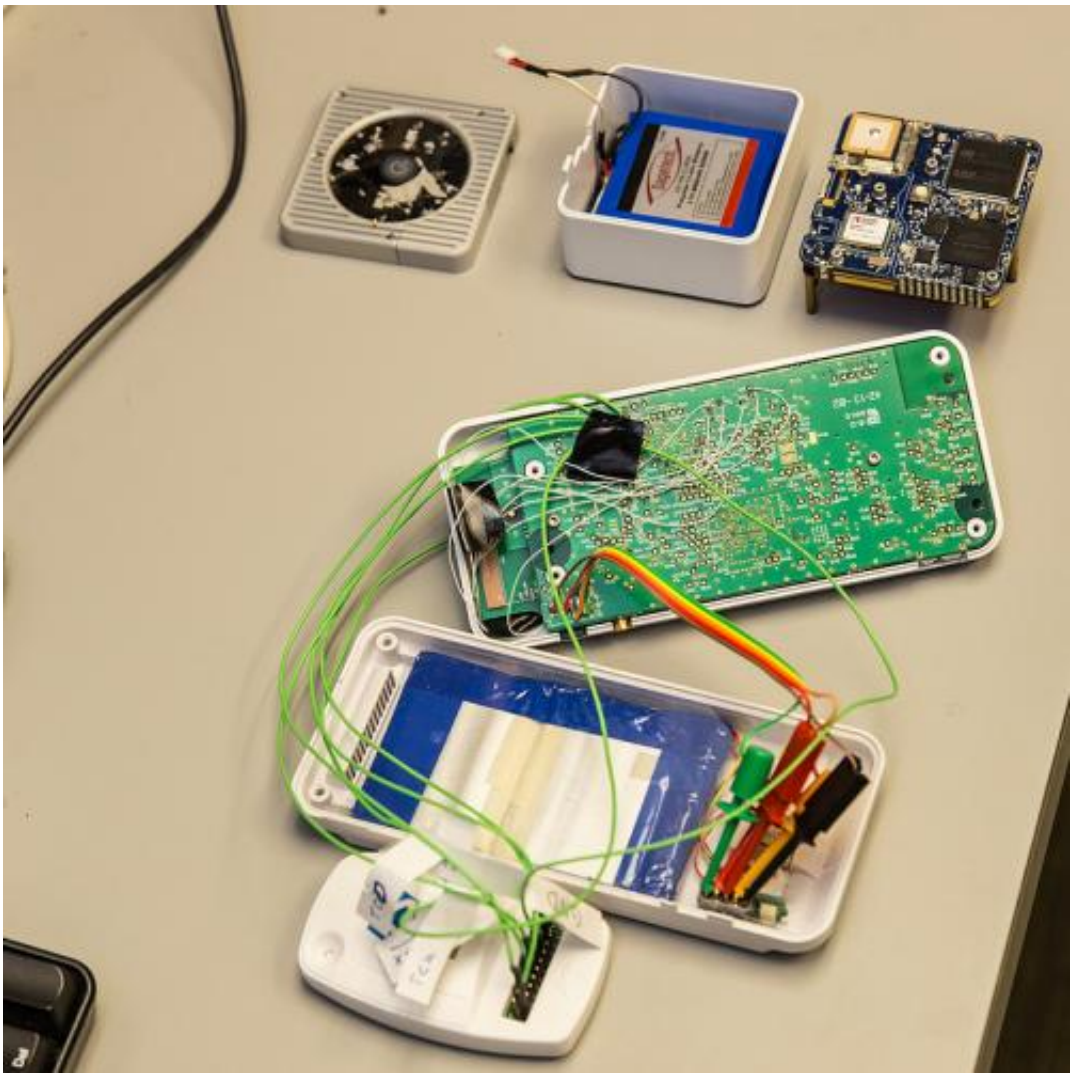
By tampering with the aircraft position, altitude, and direction indications, also known as heading, as well as weather data and positions of other aircraft displayed to the pilot, an attacker can deceive the pilot, leading them to take actions detrimental to flight safety. Factors such as visibility and pilot workload increase the likelihood of a catastrophic outcome. For example, misrepresenting aircraft position during final approach in poor weather could result in a collision with other aircraft or a crash into nearby terrain.

Researchers point to several secure design practices that can remedy the flaws they identified. Among them, cryptographically securing communication between receiver and tablet, pairing the receiver with the tablet (in the same way that Apple smart phones are paired with specific computers), signing firmware updates and requiring explicit user interaction before updating device firmware. Data such as maps and approach procedures should be downloaded to the tablet using HTTPS or digitally signed by the vendor.

Most of the systems are fairly new to the market, researchers point out. "It's a great time to make them secure from the get-go," Levchenko said.

Two of the systems allowed an attacker to replace completely the firmware,

which is home to the programs controlling the devices. Credit: Jacobs School of Engineering/UC San Diego



Top: the SageTech Clarity CL01; bottom: the Appareo Stratus 2.

More information: On the security of mobile cockpit information systems, 21st ACM Conference on Computer and Communications

Security. cseweb.ucsd.edu/~savage/papers … S14MobileCockpit.pdf

Provided by University of California - San Diego

Citation: Wireless devices used by casual pilots vulnerable to hacking, computer scientists find (2014, November 10) retrieved 24 April 2024 from https://phys.org/news/2014-11-wireless-devices-casual-vulnerable-hacking.html

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.