CERT-EU
Memo
17/05/2019 - TLP:WHITE

Wireless attacks on aircraft instrument landing systems

Reference: Memo [190517-2] Date: 17/05/2019 - Version: 1.0
Keywords: transportation, aviation, aircraft, airport, spoofing, radio signal, instrument landing systems, ILS
Sources: publicly available information

Key Points

- Modern aircraft rely heavily on several wireless technologies for communications, control, and navigation.
- Attackers could potentially change the course of a flight using commercially available equipment.
- The systems used to guide planes could be hijacked by compromising and spoofing the radio signals that are used during landing.

Summary

Researchers have devised a low-cost hack that raises questions about the security of instrument landing systems (ILS), which are used at virtually every civilian airport throughout the industrialised world. Using commercially available tools, the researchers were able to spoof airport signals in a way that causes on-board navigation instruments to falsely indicate a plane is off course. Normal training will call for the pilot to adjust the plane's descent rate or alignment and create a potential accident as a result.

One attack technique is for spoofed signals to indicate that a plane's angle of descent is more gradual than it actually is. The spoofed message would generate what is sometimes called a "fly down" signal that instructs the pilot to steepen the angle of descent, possibly causing the aircraft to touch the ground before reaching the start of the runway.

The researchers consulted a pilot and security expert during their work. Both were careful to note that this kind of spoofing isn't likely to cause a plane to crash in most cases. ILS malfunctions are a known threat to aviation safety, and experienced pilots receive extensive training in how to react to them.

The devices used for the research transmit signals that impersonate the legitimate ones sent by an airport ILS. The attacker's transmitter can be located either on-board a targeted plane or on the ground, as far as three miles from the airport. As long as the malicious signal is stronger than the legitimate one reaching the approaching aircraft, the ILS receiver will lock into the attacker signal and display attacker-controlled alignments to horizontal or vertical flight paths.

So far, the researchers could not define known ways to mitigate the threat posed by spoofing attacks. Alternative navigation technologies all use unauthenticated wireless signals and are therefore vulnerable to their own spoofing attacks. What's more, only ILS and GPS are capable of providing both lateral and vertical approach guidance. Most security issues faced by aviation technologies like ADS-B, ACARS and TCAS can be fixed by implementing cryptographic solutions. However, cryptographic solutions are not fully sufficient to prevent localisation attacks. For example, cryptographically securing GPS signals similarly to the ones used in military navigation can only prevent spoofing attacks to a certain extent. An alternative would be to implement a secure wide-area localisation system based on distance bounding and secure proximity verification techniques.

Comments

How likely is it that someone would expend the considerable amount of work required to carry out such an attack in the real world?

While it is hard to envisage the motivation for such hacks because of the amount of preparation required for carrying it out, it would be a mistake to rule them out. A report published in March 2019 found that the Russian Federation has engaged in frequent, large-scale GPS spoofing exercises that caused ship navigation systems to show they are 65 or more miles from their true location.

While ILS spoofing seems esoteric in 2019, it wouldn't be a stretch to see it become more likely in the coming years, as attack techniques become better understood and software defined radios become more common. ILS attacks don't necessarily have to be carried out with the intention of causing accidents. They could also be done with the goal of creating disruptions in much the same way rogue drones closed London's Gatwick Airport for several days last December, just days before Christmas, and then the Heathrow airport three weeks later.