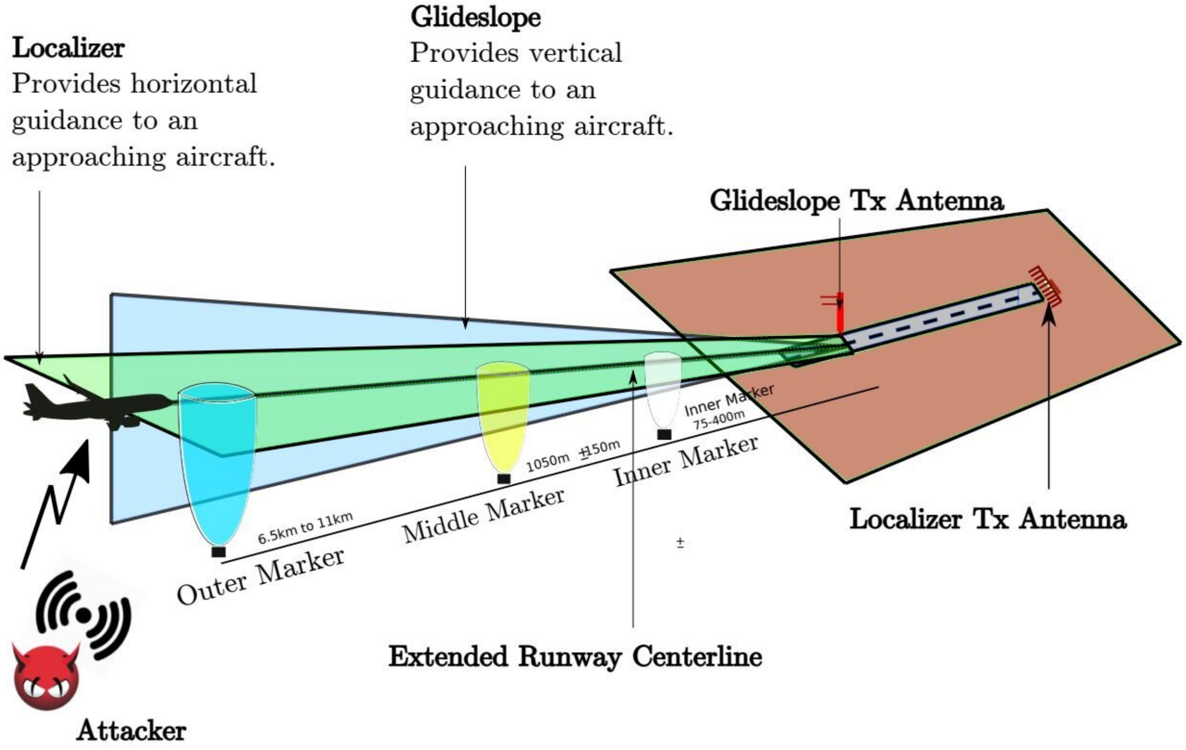
TechXplore

When an aircraft landing system is made to enter the spoofing zone

May 17 2019, by Nancy Cohen



Overview of ILS sub-systems. The ILS consists of three subsystems: i) Localizer, ii) glideslope, and (iii) marker beacons. Credit: Harshad Sathaye, et al.

Just what the airplane passenger who is always skittish does not want to hear: Radio navigation on planes for landing purposes is not secure; signals can be hacked.

In a video demonstration of the attack by researchers, "Wireless Attacks on Aircraft Landing Systems," spoofing starts automatically as soon the aircraft enters "the spoofing zone. The attacker signal is in real-time generated accounting for the maneuvers of the aircraft."

What does the spoof actually do, to trick the pilot? Dan Goodin in *Ars Technica* said the researchers can spoof airport signals in a way that causes a pilot's 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 accordingly and create a potential accident as a result."

The landing will cause last-minute abort landing decisions or even crashes in bad weather conditions, the notes added.

Their paper is titled "Wireless Attacks on Aircraft Instrument Landing Systems," by Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan and Guevara Noubir, Khoury College of Computer Sciences, Northeastern University.

The authors wrote that "resilience of the aircraft landing systems to adversarial wireless attacks have not yet been studied in the open literature, despite their criticality and the increasing availability of low-cost software-defined radio (SDR) platforms." So, that is what the researchers did—explore and show the vulnerability of aircraft instrument landing systems to wireless attacks.

One of the figures in the paper, for example, showed how the attacker's fake signal overshadowed the legitimate signal resulting in the deflection of the CDI (course deviation indicator) needle.

Why focus on landing? They wrote, "One of the most critical phases of an airplane's flight plan is the final approach or landing phase as the plane descends towards the ground actively maneuvered by the pilot."

They developed a closed-loop instrument landing system (ILS) spoofer.

(The ILS is today the de-facto approach system used by planes at a majority of the airports, said the authors, "as it is the most precise system capable of providing accurate horizontal and vertical guidance.")

Dan Goodin, *Ars Technica,* shared some observations about ILS as a precision approach system. Goodin wrote that unlike GPS and other navigation systems, "they provide crucial real-time guidance about both the plane's horizontal alignment with a runway and its vertical angle of descent. In many settings—particularly during foggy or rainy night-time landings—this radio-based navigation is the primary means for ensuring planes touch down at the start of a runway and on its centerline."

They were never designed to be immune to hackers. "Instead, pilots simply assume that the tones their radio-based navigation systems receive on a runway's publicly assigned frequency are legitimate signals broadcast by the airport operator," Goodin said.

They worked with an FAA certified flight-simulator (XPlane) incorporating a spoofing region detection mechanism, triggering the controlled spoofing on entering the landing zone, they said, to reduce detectability.

Acknowledgments of limitations: They consulted with aviation experts in setting up the experiment; in using an FAA accredited flight simulator, they sent configuration files and scripts to a licensed pilot for them to perform final approaches using the instruments and give feedback. Still, the writers discussed their setup's limitations. "We did not perform the experiments on a real aircraft."

They also said they were in the process of acquiring IRB approval to recruit commercial pilots and studying their response to the attack discussed in the paper.

Hopefully, those reading the instructive article by Dan Goodin on the researchers' work will also check out reader comments. We found a number of interesting excerpts/points of view:

"The technology referenced has been around since before digital and there is nothing new to the idea that somehow the signal could be messed with. Keep in mind most of this technology was around during the COLD WAR and everyone was well aware of adversaries thinking up ways to screw with aviation. This is one of the many reasons why the navigation systems used to land aircraft are complimentary, redundant, geographically distributed and well documented in charts so that inconsistencies can be spotted long before they are a hazard."

And another:

"ILS is known to have weaknesses, so the entire system is built to mitigate those weaknesses and to provide alternatives."

And another:

"We use ILS routinely, but we don't trust it blindly. Even a gross error check like "3-in-1", meaning 300 feet height per nautical mile to go, will tell us if we're wildly off. We also do a "final altitude check" 4-8 miles before the threshold. In case of an autoland in Low Visibility Operations, the ILS antennas are "protected", meaning the airport ensures there aren't vehicles or aircraft in the sensitive area. As an airliner pilot, you never go into an approach trusting blindly that the instrument [sic] are faultless."

More information: Wireless Attacks on Aircraft Instrument Landing Systems, aanjhan.com/assets/ils_usenix2019.pdf

Citation: When an aircraft landing system is made to enter the spoofing zone (2019, May 17) retrieved 23 April 2024 from https://techxplore.com/news/2019-05-aircraft-spoofing-zone.html