Facebook Partially Restores Privacy Feature Abused in Massive Breach

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/23-5LlGVXL4/facebook-partially-restores-privacy-feature-abused-massive-breach

---

Google Starts Tracking Zero-Days Exploited in the Wild

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/acyI3x9t7HA/google-starts-tracking-zero-days-exploited-wild

---

Microsoft Releases Attack Surface Analyzer 2.0

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/jWo9xFc6pnM/microsoft-releases-attack-surface-analyzer-20

Google’s Titan Security Keys Vulnerable to Bluetooth Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/WP1BgC59Pnw/googles-titan-security-keys-vulnerable-bluetooth-attacks

The radio navigation planes use to land safely is insecure and can be hacked

Enlarge / A plane in the researchers’ demonstration attack as spoofed ILS signals induce a pilot to land to the right of the runway.
Sathaye et al.

reader comments

79 with 62 posters participating

Share this story

Just about every aircraft that has flown over the past 50

years—whether a single-engine Cessna or a 600-seat jumbo jet—is aided by radios to safely land at airports. These instrument landing systems (ILS) are considered precision approach systems, because 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.

Like many technologies built in earlier decades, the ILS was never designed to be secure from hacking. Radio signals, for instance, aren't encrypted or authenticated. 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. This lack of security hasn't been much of a concern over the years, largely because the cost and difficulty of spoofing malicious radio signals made attacks infeasible.

Now, researchers have devised a low-cost hack that raises questions about the security of ILS, which is used at virtually every civilian airport throughout the industrialized world. Using a $600 software defined radio, 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.

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 video below shows a different way spoofed signals can pose a threat to a plane that is in its final approach. Attackers can send a signal that causes a pilot's course deviation indicator to show that a plane is slightly too far to the left of the runway, even when the plane is perfectly aligned. The pilot will react by guiding the plane to the right and inadvertently steer over the centerline.

[embedded content]
Wireless Attacks on Aircraft Landing Systems.
The researchers, from Northeastern University in Boston, consulted a pilot and security expert during their work, and all are 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. A plane that's misaligned with a runway will be easy for a pilot to visually notice in clear conditions, and the pilot will be able to initiate a missed approach fly-around.

Another reason for measured skepticism is the difficulty of carrying out an attack. In addition to the SDR, the equipment needed would likely require directional antennas and an amplifier to boost the signal. It would be hard to sneak all that gear onto a plane in the event the hacker chose an onboard attack. If the hacker chose to mount the attack from the ground, it would likely require a great deal of work to get the gear aligned with a runway without attracting attention. What's more, airports typically monitor for interference on sensitive frequencies, making it possible an attack would be shut down shortly after it started.

In 2012, Researcher Brad Haines, who often goes by the handle Renderman, exposed vulnerabilities in the automatic dependent surveillance broadcast—the broadcast systems planes use to determine their location and broadcast it to others. He summed up the difficulties of real-world ILS spoofing this way:

> *If everything lined up for this, location, concealment of gear, poor weather conditions, a suitable target, a motivated, funded and intelligent attacker, what would their result be? At absolute worst, a plane hits the grass and some injuries or fatalities are sustained, but emergency crews and plane safety design means you're unlikely to have a spectacular fire with all hands lost. At that point, airport landings are suspended, so the attacker can't repeat the attack. At best, pilot notices the misalignment, browns their shorts, pulls up and goes around and calls in a maintenance note that something is funky with the ILS and the airport starts investigating, which means the attacker is not likely wanting to stay nearby.*
>
> *So if all that came together, the net result seems pretty minor. Compare that to the return on investment and economic effect of one jackass with a $1,000 drone flying outside Heathrow for 2 days. Bet the drone was far more effective and certain to work than this attack.*

Still, the researchers said that risks exist. Planes that aren't landing according to the glide path—the imaginary vertical path a plane follows when making a perfect landing—are much harder to detect even when visibility is good. What's more, some high-volume airports, to keep planes moving, instruct pilots to delay making a fly-around decision even when visibility is extremely limited. The Federal Aviation Administration's Category III approach operations, which are in effect for many US airports, call for a decision height of just 50 feet, for instance. Similar guidelines are in effect throughout Europe. Those guidelines leave a pilot with little time to safely abort a landing should a visual reference not line up with ILS readings.

"Detecting and recovering from any instrument failures during crucial landing procedures is one of the toughest challenges in modern aviation," the researchers wrote in their paper,

titled Wireless Attacks on Aircraft Instrument Landing Systems, which has been accepted at the 28th USENIX Security Symposium. “Given the heavy reliance on ILS and instruments in general, malfunctions and adversarial interference can be catastrophic especially in autonomous approaches and flights.”

What happens with ILS failures

Several near-catastrophic landings in recent years demonstrate the danger posed from ILS failures. In 2011, Singapore Airlines flight SQ327, with 143 passengers and 15 crew aboard, unexpectedly banked to the left about 30 feet above a runway at the Munich airport in Germany. Upon landing, the Boeing 777-300 careened off the runway to the left, then veered to the right, crossed the centerline, and came to a stop with all of its landing gear in the grass to the right of the runway. The image directly below shows the aftermath. The image below that depicts the course the plane took.

Enlarge / An instrument landing system malfunction caused Singapore Airlines flight SQ327 to slide off the runway

shortly after landing in Munich in 2011.

Enlarge / The path Singapore Airlines flight SQ327 took after landing.

An incident report published by Germany's Federal Bureau of Aircraft Accident Investigation said that the jet missed its intended touch down point by about 1,600 feet. Investigators said one contributor to the accident was localizer signals that had been distorted by a departing aircraft. While there were no reported injuries, the event underscored the severity of ILS malfunctions. Other near-catastrophic accidents involving ILS failures are an Air New Zealand flight NZ 60 in 2000 and a Ryanair flight FR3531 in 2013. The following video helps explain what went wrong in the latter event.

[embedded content]

Animation – Stick shaker warning and Pitch-up Upsets.

Vaibhav Sharma runs global operations for a Silicon Valley security company and has flown small aviation airplanes since 2006. He is also a licensed Ham Radio operator and volunteer with the Civil Air Patrol, where he is trained as a search-and-rescue flight crew and radio communications team member. He's the pilot controlling the X-Plane flight simulator in the video demonstrating the spoofing attack that causes the plane to land to the right of the runway.

Sharma told Ars:

> *This ILS attack is realistic but the effectiveness will depend on a combination of factors including the attacker's*

> *understanding of the aviation navigation systems and conditions in the approach environment. If used appropriately, an attacker could use this technique to steer aircraft towards obstacles around the airport environment and if that was done in low visibility conditions, it would be very hard for the flight crew to identify and deal with the deviations.*

He said the attacks had the potential to threaten both small aircraft and large jet planes but for different reasons. Smaller planes tend to move at slower speeds than big jets. That gives pilots more time to react. Big jets, on the other hand, typically have more crew members in the cockpit to react to adverse events, and pilots typically receive more frequent and rigorous training.

The most important consideration for both big and small planes, he said, is likely to be environmental conditions, such as weather at the time of landing.

“The type of attack demonstrated here would probably be more effective when the pilots have to depend primarily on instruments to execute a successful landing,” Sharma said. “Such cases include night landings with reduced visibility or a combination of both in a busy airspace requiring pilots to handle much higher workloads and ultimately depending on automation.”

Aanjhan Ranganathan, a Northeastern University researcher who helped develop the attack, told Ars that GPS systems provide little fallback when ILS fails. One reason: the types of runway misalignments that would be effective in a spoofing attack typically range from about 32 feet to 50 feet, since pilots or air traffic controllers will visually detect anything bigger. It’s extremely difficult for GPS to detect malicious offsets that small. A second reason is that GPS spoofing attacks are relatively easy to carry out.

“I can spoof GPS in synch with this [ILS] spoofing,” Ranganathan said. “It’s a matter of how motivated the attacker is.”

https://arstechnica.com/?p=1500727

Microsoft Patches RDS Vulnerability Allowing WannaCry-Like Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/upnowTGG-fU/microsoft-patches-rds-vulnerability-allowing-wannacry-attacks

---

New Class of Vulnerabilities Leak Data From Intel Chips

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/j13q0O_lJk4/new-class-data-leaking-vulnerabilities-impact-intel-cpus

---

Twitter Collected and Shared iOS Location Data

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/20dQove6CTI/twitter-collected-and-shared-ios-location-data

---

Adobe Patches Over 80 Vulnerabilities in Acrobat Products

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/LNSxu8zLmJk/adobe-patches-over-80-vulnerabilities-acrobat-products

---

Facebook Launches Global CTF Competition

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/M4vLHgNHWcs/facebook-launches-global-ctf-competition