Comparison of Wireless Attack Impacts on Critical Avionic Safety and Guidance Systems

Dylan Miyata;
University of Hawaii at West O'ahu

Approach	Action	Action Count #	%	# Participants
1	Land	10	33.3	30
	Go-around	20	66.7	
2	Turn off	11	55.0	20
	Land	8	40.0	
	Go-around	1	5.0	
3	Turn off	1	100.0	1

Figure 1. GPWS Actions

Action	Final Selected TCAS Mode: TA/RA #	TA/RA %	TA-Only #	TA-Only %	Standby #	Standby %	Total #	Total %
Continue on route	4	13.3	10	33.3	8	26.7	22	73.3
Avoidance manoeuvre	0	0.0	3	10.0	3	10.0	6	20.0
Divert to origin	0	0.0	2	6.7	0	0.0	2	6.7
Total	4	13.3	15	50.0	11	36.7	30	100.0

Figure 2.TCAS Action After Attack

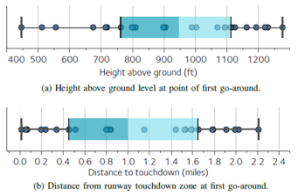

Figure 3. Go-Around Decision

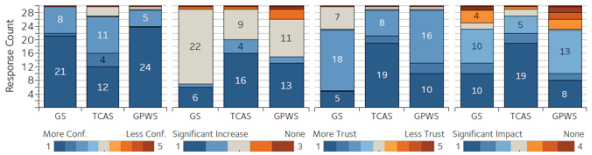

Figure 4. Overview of Pilot Responses to Attacks

Abstract

The purpose of this study is to compare the impact of wireless attacks on pilot performance due to the loss of critical safety and guidance systems during various phases of flight. These systems include: Instrument Landing System (ILS), Traffic Collision Avoidance System (TCAS), and Ground Proximity Warning System (GPWS). Such systems are critical to pilot awareness and safety during takeoff, cruise, and landing.

Introduction & Research Question

Introduction

In the paper *Safety vs. Security: Attacking Avionic Systems with Humans in the Loop* [2], researchers compared the effects of a possible attack through the use of a simulator and a group of 30 commercial airliner pilots. Each pilot is allowed a practice flight before conducting the test flights for each system failure (ILS, TCAS, GPWS). Pilots are interviewed after all flights conclude and are asked to provide a numerical rating to the following questions for each test: Confidence in their response being correct, workload difficulty due to the attack, trust in the systems due to the attack, and impact on the flight due to the attack. Additionally, yes/no responses to the following questions were also requested: would the pilot trust the system later in the flight, if the pilot felt the attack endangered the aircraft more, and if the pilot would feel the same way under real circumstances. To further understand attack effects on these systems, additional data was logged during the simulator. During ILS, a pilots decision to abort the landing to conduct a go around will be recorded in regards to altitude and distance to touchdown. For GPWS, a pilot's decision to abort the landing to conduct a go around will be recorded in regards to altitude and time since the attack is launched. For all situations, pilots may decide on different solutions to system failure. These decisions and reasoning behind such will be recorded.

Research Questions

- What is the impact of wireless attacks on pilot performance due to the loss of critical safety and guidance systems?
- Are there procedures, protocols, or safeguards in place to prevent or reduce the impact of system loss on the ground or in the air?
- What is an ideal attack scenario which may invoke in-air chaos, ground delays, or other incidents?

Hypothesis

I expect pilots to make similar decisions on each issue. However, I do think these attacks conducted under various environmental circumstances such as thick fog on the runway, high traffic areas, or mountainous terrain will yield very different results.

Research Design & Data Collection

As stated in the paper *A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems*, "In the simulator, an attacker transmits a false GS at the far end of the runway with an effective shift of 2.05 km, or 1.27 miles, creating a difference between the false and true GS of 107 m, or 352 ft. Due to the way in which ILS is implemented in the simulator software, we could not replicate also having a 'real' GS. To account for this, we operated on an assumption that the attacker transmits at a higher power than the real GS in an effort to force capture on to the false GS. The manipulation remains in place regardless of how many approaches are made. We treat the participant aircraft as if it is the first to encounter the attack, with ATC not observing previous aircraft having difficulties" [6]. Participants flew the same route, weather, 12,000 ft cruising altitude, and a flight time of 30 minutes. Each pilot is allowed a practice flight before conducting the test flights for each system failure (TCAS, ILS, GPWS).

To further understand attack effects on these systems, additional data was logged during the simulator. For ILS, a pilots decision to abort the landing to conduct a go around will be recorded in regards to altitude and distance to touchdown. For GPWS, a pilot's decision to abort the landing to conduct a go around will be recorded in regards to altitude and time since the attack is launched. For all situations, pilots may decide on different solutions to system failure. These decisions and reasoning behind such will be recorded.

Results

Figure 4 organizes the feedback from pilots with columns representing each attack and colors based upon the pilot's numerical rating. It is important to note the numerical rating range changes for each question group.

GPWS - False Terrain Alerts

With the GPWS system giving false alerts, pilots were forced to decide if a go-around was needed on the first approach. Figure 1 shows two-thirds of the pilots chose to conduct a go around due to the GPWS alerts being given during the attack. The remainder chose to disregard the alert and conduct a landing. Of the remaining 20 pilots who conducted the go-around, 11 opted to switch off the system before conducting the landing. 19 of the pilots would land successfully on the second approach. Only 1 pilot opted to conduct another go-around, switched off the GPWS system, and conducted the landing. Referring to figure 4, pilots felt the loss of reliability in GPWS created more work and impacted the safety of the aircraft.

TCAS - False Injection - Phantom Aircraft

In a simulated scenario, 30 participants were subjected to a false injection attack. Of the participants, figure 2 depicts how each setup TCAS and responded to TCAS alerts. As shown in figure 2, 20% of participants did perform the RA avoidance maneuver while 73.3% continued with the flight. Two participants diverted back to their airports of origin. "27 (90%) pilots felt that the attack had at least 'some impact', with 19 (63%) feeling that it had 'significant impact'. This was coupled with 29 (97%) feeling that there was at least 'some increase' in workload" [6]. 29 pilots stated some distrust in the TCAS system as the scenario played out. As stated earlier in this paper, pilot distrust in TCAS was a primary factor in making false injection a high risk.

Glide Slope - False ILS GS Lobes

The glideslope spoof is perhaps the most dangerous of the attacks since the attacker does not need to disable or destroy the original signal. In Figure 3, we can see there is a noticeable spread in pilot action taken during approach. As noted in the paper Safety vs. Security: Attacking Avionic Systems with Humans in the Loop, "On encountering the attack, 4 (13.3%) participants chose to land anyway on account of having a good visual picture. Of the 26 (86.7%) participants choosing to go around, three went around a further time" [6]. Additionally, some pilots upon noticing the GS issue conducted different actions prior to landing. These actions are listed below:

VHF Omnidirectional Range approach.	1 Pilot
Surveillance Radar Approach (SRA), which relies on higher involvement with ATC.	2 Pilots
Localizer only approach (LOC DME)	8 Pilots
Dropped ILS completely, and used an Area Navigation (RNAV) approach, which is based on GPS.	9 Pilots
Flew a visual approach due to good conditions.	6 Pilots

Out of all attack responses, the glide slope spoof created the greatest variety in pilot response. In addition to the spread out go-around height and distance to runway, pilots also noted more severe weather would have produced a greater challenge to overcome. Referring back to Figure 4, 13 pilots did report a higher impact and 22 reported slight workload increases due to the GS issue. However, 19 pilots did say the attack placed the aircraft in more danger.

Discussion

"As recently as September 2018, the pilots of Air India flight AI-101 reported an instrument landing system (ILS) malfunction and were forced to do an emergency landing. Even worse, TCAS, ACARS, and a majority of other systems that aid a smooth landing were unusable. Furthermore, NASA's Aviation Safety Reporting System indicate over 300 ILS related incidents where pilots reported the erratic behavior of the localizer and glideslope– two critical components of ILS. ILS also plays a significant role in autoland systems that are capable of landing aircraft even in the most adverse conditions without manual interference" [5]. This example pulled from the paper *Wireless Attacks on Aircraft Instrument Landing Systems* demonstrates an extreme scenario where the loss of critical systems can force an emergency. This project aimed to compare the impact of wireless attacks on three such systems: ILS, TCAS, and GPWS. Pilots tended to take similar actions but, in other cases such as ILS, pilot responses varied far more. This proved to be no issue as all pilots landed successfully at some point. Below are pilot response to if they would conduct the same actions in a real aircraft:

- GPWS, 27 (90.0%) would do the same, and the remaining three would go around in the same scenario again. [7]
- TCAS, 30 (100.0%) would do the same.[7]
- Glideslope, 28 (93.3%) would do the same with the remaining two opting to go around and revert to RNAV.[7]

The critical detail to note is the redundancy of protocols and systems. The ILS and GPWS spoof can easily be averted by switching to a manual landing. As mentioned earlier in this paper, ILS approaches can take on different categories based on airfield capabilities and approach conditions. Under CAT I and CAT II, it is likely pilots will be able to see the PAPI system placed near the runway from a farther distance. Since the PAPI does not rely on any signals, pilots can trust the information being relayed is correct for a manual approach. Additionally, ILS and PAPI ground systems are physically protected areas. Gaining access without detection would not be easy. TCAS issues could be averted easily through the use of ATC assistance on traffic location or by switching the system mode, an action most pilots took.

However, much like the Air India flight AI-101, a worse case scenario where a CAT III approach in severe weather with no systems would likely prove disastrous. It would be unlikely the flight crew would be able to spot the runway, terrain, or PAPI until a very close visual range was achieved. Additionally, heavy weather may make a physical intrusion on the ground far more likely. Attackers may be able to set up false ILS antennas and possibly alter the PAPI. Assuming such factors are achieved, the flight crew would be flying blind. In this sort of scenario, it would be difficult to conduct a go-around and may result in a runoff or crash.

Conclusions

It is safe to say that the current systems, protocols, and procedures enforced by the FAA are capable of preventing such incidents from occurring. Disruptions, delays, and increased confusion amongst aircraft will happen under such attacks. However, I do not believe these attacks are capable of causing a significant accident. Even under the proposed ideal attack scenario, an accident would only occur under ATC and or pilot error.

Contact

Dylan Miyata
University of Hawaii at West O'ahu
Email: dmiyata7@hawaii.edu
Phone: (808) 352-4184

References

1. Airbus. (2001). Getting to Grips With Category II and III Operations. (STL 472.3494/95). https://www.skybrary.aero/bookshelf/books/1480.pdf
2. Berges, P. M. (2019). *Exploring the vulnerabilities of traffic collision avoidance systems (TCAS) through software defined radio (SDR) exploitation* (Doctoral dissertation, Virginia Tech).
3. Berges, P. M., Shivakumar, B. A., Graziano, T., Gerdes, R., & Celik, Z. B. (2020, June). On the Feasibility of Exploiting Traffic Collision Avoidance System Vulnerabilities. In *2020 IEEE Conference on Communications and Network Security (CNS)* (pp. 1-6). IEEE.
4. Hannah, J., Mills, R., Dill, R., & Hodson, D. (2021). Traffic collision avoidance system: false injection viability. *The Journal of Supercomputing*, 1-24.
5. Sathaye, H., Schepers, D., Ranganathan, A., & Noubir, G. (2019). Wireless attacks on Aircraft Landing Systems. *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. https://doi.org/10.1145/3317549.3326298
6. Smith, M., Strohmeier, M., Harman, J., Lenders, V., & Martinovic, I. (2019). Safety vs. security: Attacking avionic systems with humans in the loop. *arXiv preprint arXiv:1905.08039*.
7. Smith, M., Strohmeier, M., Harman, J., Lenders, V., & Martinovic, I. (2020). A view from the cockpit: Exploring pilot reactions to attacks on Avionic Systems. *Proceedings 2020 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2020.23022
8. U.S. Department of Transportation Federal Aviation Administration. (2011). Introduction to TCAS II Version 7.1 (HQ-111358). https://www.faa.gov/documentlibrary/media/advisory_circular/tcas%20ii%20v7.1%20intro%20booklet.pdf
9. U.S. Department of Transportation Federal Aviation Administration. (2017). Instrument Procedures Handbook. (FAA-H-8083-16B). https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/instrument_procedures_handbook/media/faa-h-8083-16b.pdf
10. U.S. Department of Transportation Federal Aviation Administration. (2018). Procedures for the Evaluation and Approval of Facilities for Special Authorization Category I Operations and All Category II and III Operations. (Order 8400.13E). https://www.faa.gov/documentLibrary/media/Order/Order_8400.13E.pdf