IT-Security in modern aviation

Timo Skrobanek
Heidelberg University
IT-Security Seminar Heidelberg, Germany

ABSTRACT

Aviation security extends far beyond the physical act of flying. Recent years have shown, that airlines and other actors in the aviation sector became increasingly interesting to groups with malicious intentions - e.g Hacker or Terrorists. Airports and airlines represent high-value targets for cyberattacks or incidents by third party.

This paper goes over points of interest in aviation, different approaches to interfere with aircrafts or infrastructure and the reaction of the ICAO and EUROCONTROL.

1 INTRODUCTION

Regarding It-Security in the aviation sector, it is helpful to divide the field into three main areas, each with its own specific physical and technical security requirements.

At first General Aviation (GA) which considered for anything not commercially related to aviation. This includes small aircraft (e.g Cessna 172). This sector is mostly open to everyone and has the least security measures. Obviously, when heading to a large airport like Frankfurt, Munich, etc. there are more layers of security but when operating on local airfields you won't face the same security layers.

Second, is commercial aviation, which has the greatest impact on all of us. Just in the USA, there are approximately 44.000 flights/day [6]. This marks about 40% of all flights per day. Given the scale and the large number of passengers transported daily, it is crucial to implement robust security measures. These measures aim to address potential errors, such as human error or to prevent incidents

Third, is military aviation. Since this sector is highly classified - publicly known countermeasure would be dangerous for the individual military - there is not much information about Cybersecurity and security aspects in general.

2 POINTS OF INTEREST IN AVIATION

With these sectors in aviation, we now identify potential points of interest for malicious actors as possible points of failure within each domain.

2.1 ATC/Communication

One might try to interfere with the communication systems between Air Traffic Control (ATC) and the pilots/aircraft. Since communication is crucial especially close to airports, - Managing of arriving and departing aircraft, handling ground movement, etc. - It becomes very dangerous if communication is not possible.

2.2 Passenger booking systems

Airlines handle and store passenger information like other sectors and companies. This results in the possibility of data leaks.
Another problem for the airline could result in a blockage of the system. This might force the airline to temporarily stop operating, since there are no sold tickets [7].

2.3 Airport infrastructure

Airports are large and complex infrastructures composed of numerous interdependent systems. While many of these systems are directly related to physical security, IT security often operates in the background and is less visible. However, for actors with malicious intention, airports present several potential vulnerabilities. One possible objective could be to smuggle unauthorized items - such as jamming devices or other equipment on board an aircraft. Another threat scenario involves the manipulation of digitally transmitted data, such as altering the calculated fuel or weight data. Such changes could have serious consequences for flight safety.

2.4 Aircraft

We all know an aircraft as a flying machine with flight control systems, a cockpit and passenger area. Today this perspective isn't accurate anymore. A modern aircraft like the ones built by Boeing or Airbus are more likely a flying computer. Given the complexity of all the systems in an aircraft one could try to interact with e.g autopilot, flight controls or other crucial onboard systems [2].

3 CYBERTHREATS ON THE GROUND

Aviation involves far more than simply transporting people or goods from one point to another. Before a plane can even take off, numerous background processes must take place. Each of them contributing either to flight safety or to the efficient and economic execution of operations. As previously mentioned, airports alone offer a wide range of potential targets. This not only applies to airports. Back in 2020 more than 60% [5] off all attacks where targeting airlines with the goal to steal customer data or shutdown operational systems what caused airlines to stop operating temporary.[7, "Delta Airlines locked access for customer to accounts"]
Obviously airlines are not the only potential targets but probably the most interesting ones. Below is a figure showing more incidents including other targets.

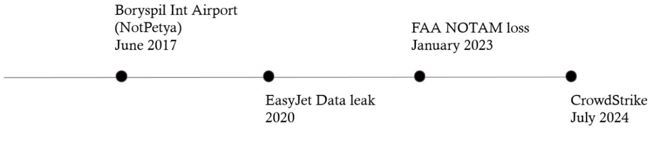
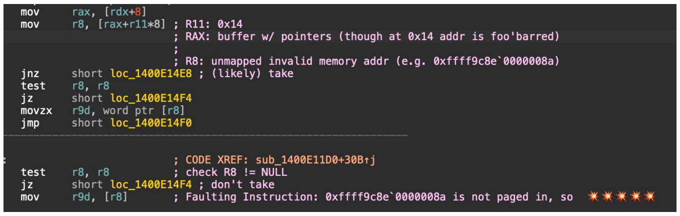


Figure 1: A selection of some incidents

3.1 CrowdStrike outtage

One particularly impact full incident was the case involving CrowdStrike. The company specializes in developing antivirus and cybersecurity solutions for B2B clients and holds a significant share of the cyberscecurity market [4]. As a major provider in the industry, any disruption to their services can have wide reaching consequences for organizations that rely on their protection.
In 2024, CrowdStrike released routine updates for configuration files and malware signatures. [3, incident explained by CrowdStrike] However, prior to this update, faulty code had already been introduced into the system. Until this moment, the problematic segment had remained undetected and was not executed during runtime. With the new update, this section of code became relevant, leading to the driver crashing and not being able to restart the whole system, since it remained in the well known "Blue-screen of death". [11, Easier explaination]



```
mov     rax, [rdx+8]
mov     r8, [rax+r11*8] ; R11: 0x14
                        ; RAX: buffer w/ pointers (though at 0x14 addr is foo'barred)
                        ;
                        ; R8: unmapped invalid memory addr (e.g. 0xffff9c8e`0000008a)
jnz     short loc_1400E14E8 ; (likely) take
test    r8, r8
jz      short loc_1400E14F4
movzx   r9d, word ptr [r8]
jmp     short loc_1400E14F0
---------------------------------------------------------------

                        ; CODE XREF: sub_1400E11D0+30B↑j
test    r8, r8          ; check R8 != NULL
jz      short loc_1400E14F4 ; don't take
mov     r9d, [r8]       ; Faulting Instruction: 0xffff9c8e`0000008a is not paged in, so ✴✴✴✴✴
```

Figure 2: Reproduced segment by Patrick Wardle [10]

3.2 Impact to aviation

The CrowdStrike incident demonstrated how the security standards of a single company can have significant impact on global operations. The failure led to substantial costs for airlines, airports and passenger. In total, around 5000 flights were delayed and airlines faced numerous operational challenges [13]. In some cases, boarding passes had to be issued by hand and missing arrival/departure displays further complicated daily routines.
Globally, approximately 1% of all windows-based-systems were affected - amounting to around 8.5mio devices [13]. So obviously the questions rise for me:

"Are there further hidden problems?"

4 POSSIBILITY OF HACKING AIRCRAFTS

As previously discussed, modern aircraft should be viewed as large, complex computers [2]. From this perspective, one might consider the possibility of hacking attempts that target the aircraft directly. In some cases, these concerns are justified. Parts of the aviation industry still rely on standards dating back to the 1970s [1].

4.1 Aircraft - A flying computer

Let us take a modern aircraft such as the Airbus A320 as an example. Airbus equips its aircraft with a system known as "Fly by wire" [2]. This technology enables a complete decoupling of the cockpit controls from the physical control surfaces of the aircraft. In other words, the pilot's inputs are not transmitted mechanically but are instead processed and relayed electronically. Before any input from the pilot is actually executed by the aircraft, it is first analyzed by multiple onboard computers. These computers determine whether the command falls within the aircraft's operational limits [2]. For instance, if the pilot pulls back on the side-stick to raise the aircrafts nose, the system checks parameters such as the current G-load and the angle of attack. If executing the input would result in exceeding these limits the system will intervene and prevent the command from being fully carried out.

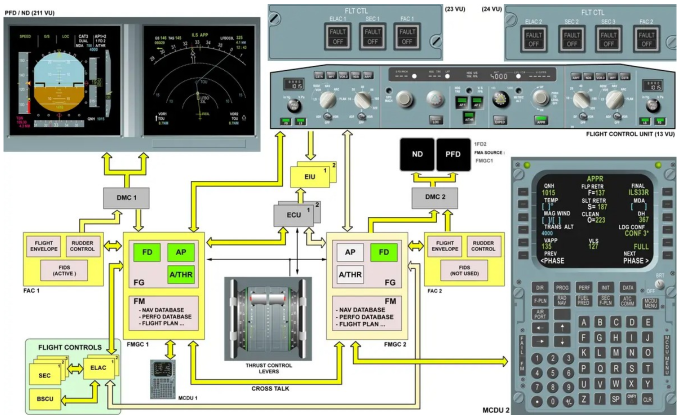


Figure 3: Complexity of an FBW aircraft - e.g A320 [2]

Of course this only one example for the flight controls. There are many other systems, also being checked by redundant computers like the autopilot, engine monitoring and so on [2].

4.2 How realistic is such an attack?

While the idea of hacking directly into an aircraft's control system may seem like something out of a movie, the risk cannot be entirely dismissed - Affecting the systems and displaying wrong data is possible and we'll discuss this in the next part of this paper. Modern aircraft are highly complex and although systems like fly by wire are designed with multiple layers of redundancy and security, they are not entirely immune to cyberthreats since they are basically computer systems, meaning there is no 100% security.
That said, critical systems in commercial aviation are typically isolated from non-critical systems [2]. Another major challenge for potential attackers is gaining access to these systems in the first place. Unless someone is already working within the aviation industry, it is extremely difficult to get close to an aircraft and even if one is successfully there, the computers are still separated from both passenger cabin and the cockpit.
Finally it's really hard to access the aircraft via this way, so there are other possibilities which we'll have a look on now.

5 IN FLIGHT CYBERTHREATS

In recent years, it has become increasingly clear that threats to aviation can arise even when the attacker is not in the immediate vicinity of the aircraft [5]. From missile strikes in conflict zones to signal jamming and data manipulation within the cockpit [8], there is now a broad range of methods that pose serious risks to commercial aviation.

5.1 GPS jamming and spoofing

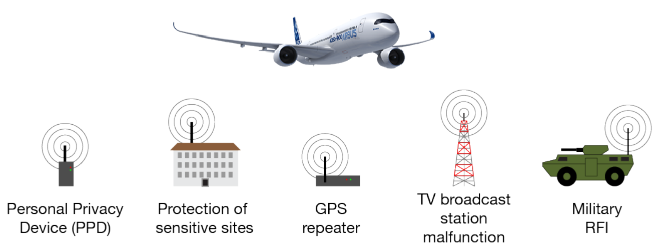

Personal Privacy Device (PPD)
Protection of sensitive sites
GPS repeater
TV broadcast station malfunction
Military RFI

Figure 4: Possible sources for jamming [1]

One threat that is currently gaining global significance is GPS-Jamming and Spoofing. Both techniques can produce similar effects in the cockpit by interfering with satellite-based navigation [1]. The first option is to completely overwrite In both cases the result will be wrong data shown the pilots, starting with wrong positioning data, not accurate working clocks or even wrong indications of the GPW-system (Ground proximity warning system).

5.2 Countermeasures

All those indication on their own, would not lead to an incident or crash at all, but just think of bad weather conditions, when pilots have to trust their systems or when performing a highly accurate autopilot landing. In general an incident is always a combination of many failing parts. Doesn't matter if human errors or system errors.

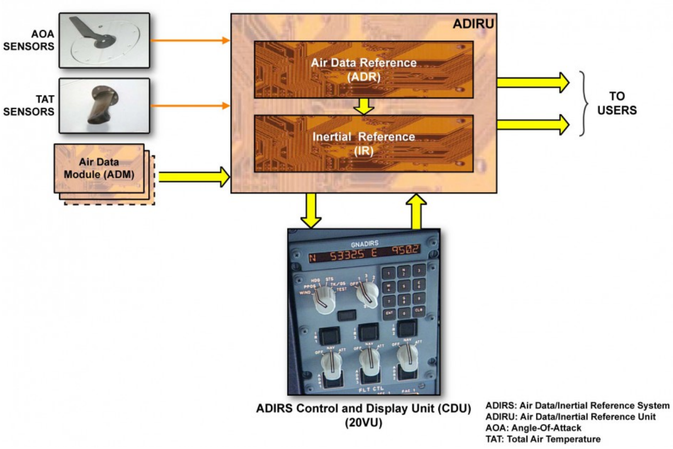

AOA SENSORS
TAT SENSORS
Air Data Module (ADM)
ADIRU
Air Data Reference (ADR)
Inertial Reference (IR)
TO USERS
ADIRS Control and Display Unit (CDU) (20VU)
ADIRS: Air Data/Inertial Reference System
ADIRU: Air Data/Inertial Reference Unit
AOA: Angle-Of-Attack
TAT: Total Air Temperature

Figure 5: Backup-system [1]

Modern aircraft are equipped with redundant systems designed to handle nearly any type of failure scenario. While these backup systems ensure continued operation, they often come with certain limitations. In the case of GPS jamming, one such alternative is the ADIRU (Air Data Inertial Reference Unit System) [1]. This system calculates the aircraft's position based on initial coordinates entered into the FMS (Flight management system) while the aircraft is still at the gate. From that point onward, the ADIRU uses a combination of accelerometers and gyroscopic sensors to continuously measure movement in all directions, allowing the system to estimate the aircraft's current position. Since there is a small offset in each calculation this system is reliable for on route navigation but not for navigation based approaches.

5.3 Where does it happen?

This type of threat is particularly prevalent in conflict zones around the world [8]. However, in recent years, GPS jamming and spoofing incidents have increasingly been reported in European airspace as well. [8]

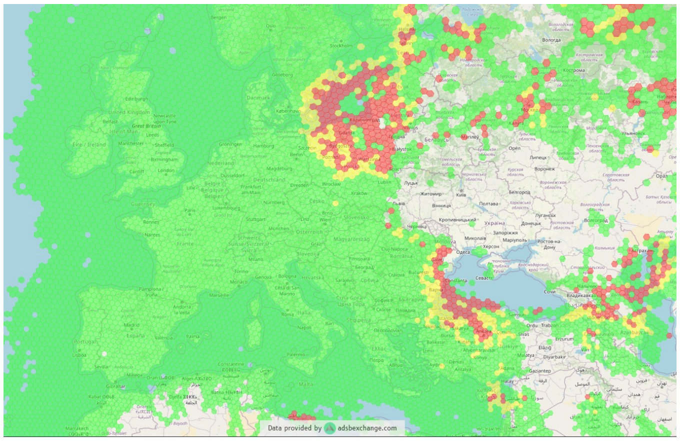


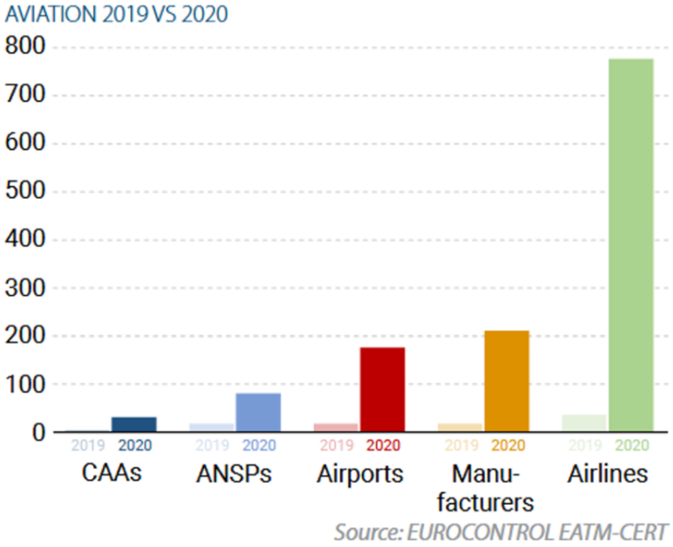
Figure 6: GPS interference on 10th august 2025 [8]

Due to the high number of occurrences, the issue has, in same cases become unavoidable for certain flights. Aviation relies on predefined air routes and rerouting may either be economically unfeasible or operationally impossible. This is forcing airlines and authorities to adapt to with mitigation strategies and heightened situational awareness.

6 RESULTS AND FINDINGS

Within only one year the interest in taking influence to the aviation sector increased heavily. The reasons for this drastic increase are discussed in the paper of EUROCONTROL [5].

6.1 Actors and responsible members



Source: EUROCONTROL EATM-CERT

Figure 7: Development of cyberthreats [5]

The aviation industry became aware of digital threats relatively early. However, for many years, there were no unified regulations or cybersecurity standards across the sector. As a result, airlines often developed their own internal policies and practice to address emerging risks. For example in 2015 United Airlines launched a "Bug and Bounty" program aimed to improve the security of their systems [12].

6.2 ICAO Cybersecurity Action Plan

One important step toward standardization was taken by the ICAO (International Civil Aviation Organization), which published the Cybersecurity Action plan [9] back in 2020. This plan outlines a set of guidelines and recommended practices for airports, airlines and aviation related staff in general.

This plan lays the foundation for international cooperation across the aviation industry. It establishes common rules for incident management, emergency planning and the training of aviation personal in cybersecurity best practice.

In total the plan outlines 51 implementations, aimed at strengthening global cyber resilience in aviation [9].

REFERENCES

[1] Airbus. 2019. *GNSS Interference.* https://safetyfirst.airbus.com/gnss-interference/ Accessed: 2025-08-10.

[2] AviationHunt. 2014. *ATA 22: Airbus A320 (Technical Notes).* Technical Report. AviationHunt. https://www.aviationhunt.com/airbus-a320-ata-22/ Accessed: 2025-08-10.

[3] CrowdStrike. 2024. *Channel File 291 Incident.* https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/ Accessed: 2025-08-10.

[4] CrowdStrike. 2025. *About us.* https://www.crowdstrike.com/en-us/about-us/ Accessed: 2025-08-10.

[5] EUROCONTROL. 2021. *Think Paper on Cyberthreats.* Technical Report. EUROCONTROL. https://www.eurocontrol.int/sites/default/files/2021-07/eurocontrol-think-paper-12-aviation-under-cyber-attack.pdf Accessed: 2025-08-10.

[6] FAA. 2025. *Air Traffic By The Numbers.* https://www.faa.gov/air_traffic/by_the_numbers Accessed: 2025-08-9.

[7] Forbes. 2025. *These 3 Airlines Were Cyberattacked In The Last 3 Weeks—Here's What We Know.* https://www.forbes.com/sites/suzannerowankelleher/2025/07/02/3-airlines-cyberattack-qantas-westjet-hawaiian/ Accessed: 2025-08-10.

[8] GPSJAM. 2025. *Map for GPS jamming.* https://gpsjam.org/ Accessed: 2025-08-10.

[9] International Civil Aviation Organization (ICAO). 2023. *Cybersecurity Action Plan.* Technical Report. International Civil Aviation Organization. https://www.icao.int/aviationcybersecurity/Pages/default.aspx Accessed: 2025-08-10.

[10] Patrick Wardle. 2024. *Air Traffic By The Numbers.* https://x.com/patrickwardle/status/1814343502886477857 Accessed: 2025-08-11.

[11] The Morpheus Tutorials. 2024. *Crowdstrike Ausfall: Technische Analyse und Lektionen (German).* https://www.youtube.com/watch?v=Y5wGWIAPnbc&t=746s Accessed: 2025-08-10.

[12] United Airlines. 2015. *Vulnerability Disclosure Program.* https://www.united.com/en/us/fly/united-airlines-vulnerability-disclosure-program.html Accessed: 2025-08-10.

[13] wtwco. 2024. *How did the CrowdStrike outage affect aviation operations?* https://www.wtwco.com/en-gb/insights/2024/09/how-did-the-crowdstrike-outage-affect-aviation-operations Accessed: 2025-08-10.