Analysis of cyber vulnerabilities in civil aviation and recommendations for their mitigation

Evgeni Andreev, Dimitar Dimitrov

Naval Academy "Nikola Vaptsarov", Asst. Prof. in Department of Information Technology, Faculty of Engineering, Varna, Bulgaria, e.andreev@naval-acad.bg

Naval Academy "Nikola Vaptsarov", Cybersecurity student, Varna, Bulgaria, dimitar@gmx.us

Abstract: The article reviews the main attacks which affect aviation. The weaknesses in protocol codes and the threats are highlighted. Trends related to security problems and vulnerabilities at airports and air bases are presented. An overview and analysis of some of the most notorious aviation hacking attacks and their consequences is reported. The paper focuses on a possible man in the middle attack which can compromise the link between the aircraft and the communication base. A demonstration of man in the middle with the ASTERIX protocol is presented. As a result of the problem analysis, recommendations are proposed to mitigate these vulnerabilities and their impact. Innovative protection methods involving artificial intelligence and machine learning are outlined.

Keywords: aviation, protocols, cybersecurity, cyber attacks, artificial intelligence

1. Introduction

Although the COVID-19 pandemic has affected tourist aviation for years to come, together with all other branches of aviation, a total of $3.5 trillion is still generated to the world GDP. GDP is expected to grow by another $750 billion in 2021 [1]. Aviation is one of the main engines of the modern economy and one of the main pillars of any country's development. Aviation has various branches, both in the business industry and in the commercial, military, humanitarian, tourism and research industries. The success of aviation in business, tourism and commerce over other methods of transportation is due to the speed with which it is carried out the intended and many times faster, compared to sea transport. One of the most important factors in the efficiency of aviation in these areas is the advanced technology that enables its development. As technology advances, the logistical overload of ground control involving human intervention decreases. This allows for optimal air transport transfers so as to save time. Before the advent of modern technologies for air traffic control and logistics operations, additional time was needed to calculate and reconfigure flight plans. The advent of technology also brings risks of new threats that security professionals face every day. The risks of a technology outage or hacker attack could be fatal to some of the companies that rely entirely on technology and could result in tens of billions of dollars in losses. The speed at which malware and methods are improving leads to them quickly adapting to countermeasures taken by security professionals. These threats threaten both the metaverse and the physical world. If radar systems are compromised, tracking aircraft will be uncertain and dangerous. A solution to the problem is the creation of new protocols and data encryptions to limit the interference of malicious actors.

2. Common attacks in aviation.

Frequency eavesdropping is common as the tools needed to do so are easily available. Communication channels are standardized on known frequencies, these are publicly available in aeronautical information publications. Since VHF radio communication is not encrypted, VHF communications are vulnerable to

eavesdropping. Such as the main protocol in aviation Automation Device Specification – Broadcast (ADS-B) uses an unencrypted way to broadcast the information and is a publicly known protocol [2]. The unencrypted information allows sites such as flightradar24.com in Figure 1 and planefinder.net to make information about a large amount of public and military aircraft available online. This in itself is not dangerous, but provides the necessary information for malicious activities.

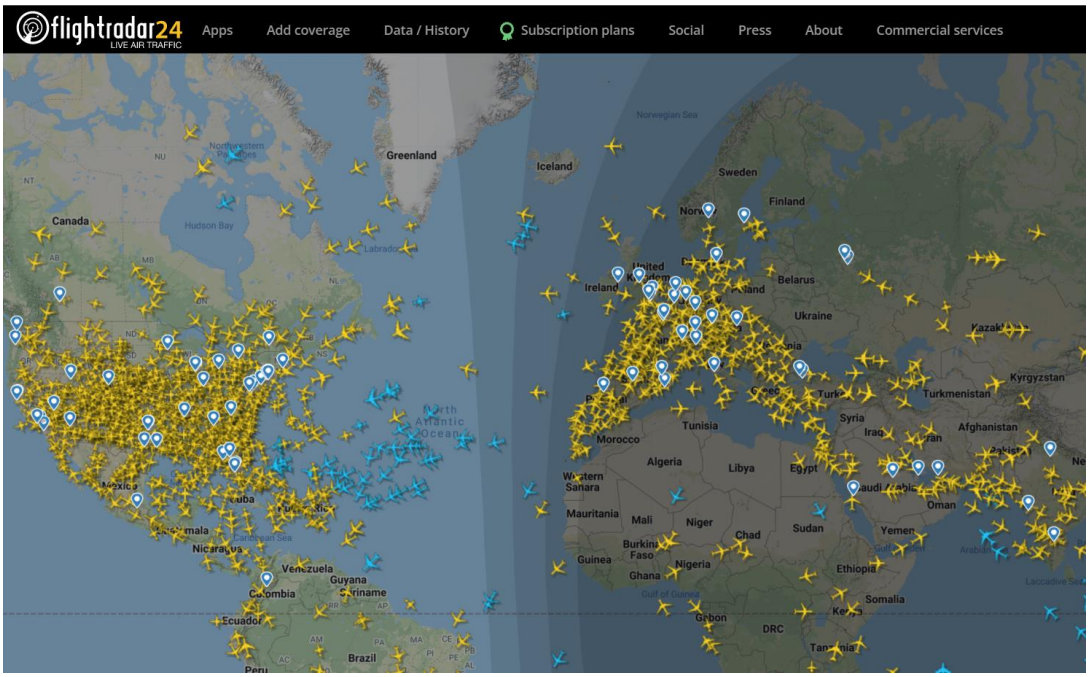

Figure 1. The website flightradar24.com, where a large number of civilian aircraft and some military aircraft can be tracked.

Jamming is another attack that is easy to perform. The requirements for implementing this attack are that it be executed from approximately close range to the communications base they intend to jam, or needs a strong power supply. This attack works by the method of Denial-of-Service (DoS) attacks - sending a continuous and large number of high frequency signals that fill the memory of the communication elements that try to process each signal [3]. As a consequence of filling the working memory with malicious and "junk" information and overloading it with processing, radar systems cease operation. It can affect most secondary radar systems as well as most non-military primary radar systems. Localization of this type of attack is done quickly because the frequency it emits is obvious to sensors and can be traced to the primary source. It is also possible to do this through an unmanned aircraft type system, which would also leave fewer traces. Such an attack was executed in 2015 by the Russian state-sponsored APT (advanced persistent threat) group Pawn Storm [4]. The consequences were hundreds of planes unable to take off in a 5 day period as the Swedish ATS (air traffic control) was constantly jammed.

One of the most dangerous attacks is Man in the middle. This is the attack that detects the connection between aircraft and ground control, modifies the connection and sends malicious code. Some of the most common methods of Man in the middle attacks are: ARP poisoning, DNS Spoofing, GPS Spoofing, Port Stealing and DHCP Spoofing. Spoofing attacks send a signal with information that works on the same principle as the data transmission protocol. The difference is that it sends fake information by impersonating the real sender. The GPS Spoofing method is one of the most impactful attacks as it a more intelligent form than jamming and jamming. This type of attacks aims to make the receiver take wrong

coordinates, which makes it confuse the aircraft navigation system completely [5]. Data link layer has no implemented methods for identification and authentication of received command signals. This allows a spoofing attack to be carried out on the radio transmitters located nearby, sending false GPS signals into the target receiver. In this way, the attacker can control the navigation system of the aircraft and set his own target courses.

In combination with spoofing attacks and message deletion attacks it is possible to manipulate the ATC (Air Traffic Control) console. When a jamming signal is sent fast enough to cause constructive interference, it causes a large enough number of errored bits so that the received message is detected as corrupt and deleted. By overlaying the spoofed message with a higher power, this enables a spoofing attack to be sent.

Fake websites and phishing attacks related to airlines are the most common cyber attacks in 2020, accounting for 87% of reported cyber attacks in the airline industry, as can be seen in Figure 2. They are cheap, easy to spread and successful. Their main purpose is to steal data and sensitive information from airports and airbases, and from people who are lured by phishing sites. Phishing attacks can also spread malware that is more dangerous to an airport's IT infrastructure. In a ransomware attack, this could paralyze an airport's operations for days, even weeks.

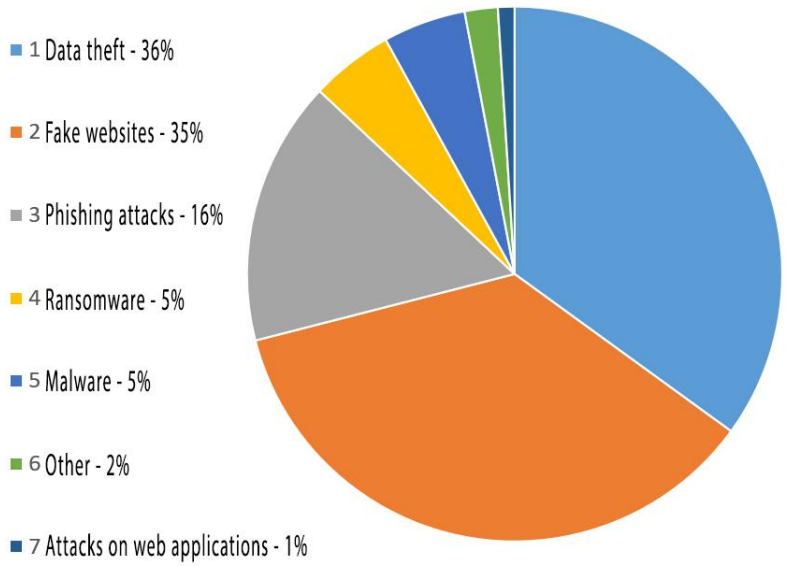

Figure 2. Chart of the most common attacks in the airline industry in 2020 [6].

3. Analysis of attack types and problems in civil aviation.

One of the first examples of a hacker attack that disrupted flights was in 2015. Following a DDoS attack on LOT Airport in Poland [7], many of the systems responsible for important flight operations were taken offline. The attack resulted in the suspension of 10 flights and directly affected over 1500 passengers. There is no evidence of data leakage or compromise of internal systems.

One of the most recent attacks on aviation infrastructure has been recorded in 2019 at the European International Airport. While installing a new Cyberbit anti-virus program, the Monero malware was detected, the purpose of which is to use the victim's computer configuration to be added to cryptocurrency

mining cluster programs. After the Cyberbit report, it is found that more than 50% of the airport's systems are infected with this malware. In order to evade the airport's defenses, the Monero crypto malwareer uses PAExec, a version of Microsoft's PsExec, a program for remotely executing processes on other systems. This enables the malwareer to execute as a system mode, allowing it to gain maximum user privileges, i.e., use the full allowed resources of the airport's systems. Another feature that PAExec gives is priority over other programs to use the resources of the computer systems. In order to evade antivirus programs at the airport, a Reflective Dynamic-Link Library (DLL) type attack is used. It allows the injection of a malicious Dynamic-Link Library that is loaded into memory rather than the hard disk. This allows stealth persistence and evasion of antivirus sensors. The malicious activity detection data shown in Figure 3 and Figure 4 were taken using Google's online virus scanning tool, VirusTotal. VirusTotal scans files across many antivirus companies, indicating how many of them detect malicious activity and what type it is. An experiment was done by scanning the crypto malware Monero through VirusTotal. Figure 3 shows the result from the fall of 2019 where more than 57 antivirus did not detect malicious activity and only 16 were able to detect the malicious file . Figure 4 shows how as the number of incidents related to the Monero malware increases, the number of antiviruses not detecting malicious activity is 26 out of 69 as of March 2022. According to official data, the consequences of this attack are a slowdown of computer systems and an increase in power consumption. However, this malware is classified as a medium-level attack vector as it enables the attacker to perform a wide range of actions. It enables downloading other malicious payloads and compromising entire networks. In the worst case, this type of attack would compromise critical operational networks, from runway lights to the airport transportation system.

Figure 3. Malware file analysis by VirusTotal. September 2019 [8].

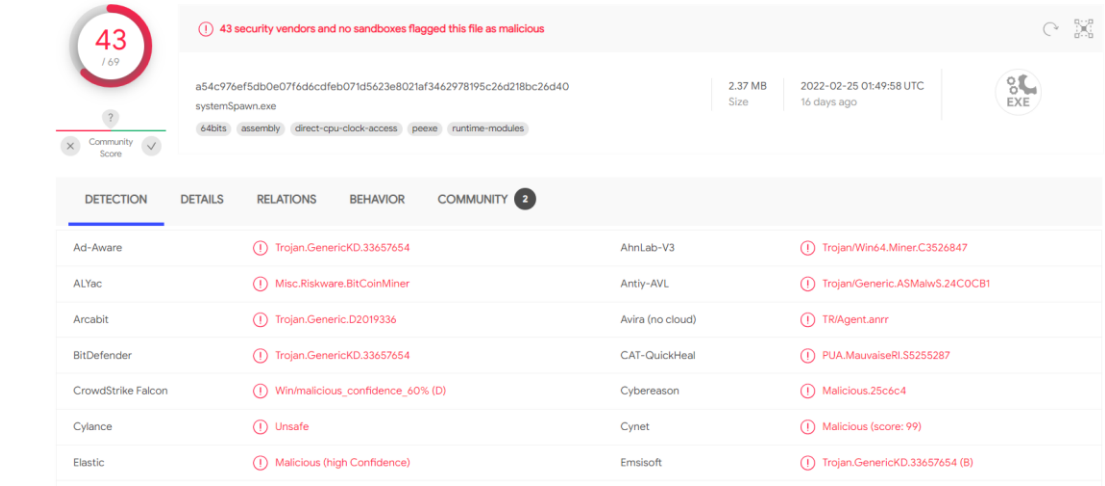

Figure 4. Malware file analysis by VirusTotal. March 2022.

A sample file [9] for eavesdropping traffic over the ASTERIX protocol is examined. The file has been analyzed using Wireshark network protocol analyzer and capture software. In order for an attacker to be able to read the information transmitted between an aircraft and the control center, they must tap into the network between them. The aircraft sends information to the ground radar. The information is processed and sent, via the ASTERIX protocol (All Purpose STructured Eurocontrol SuRveillance Information Exchange) through many network devices to its final destination - the control center. There the

information is processed and displayed to make decisions. The problem arises in the communication path from the encapsulation of the information, via the ASTERIX protocol, to the decapsulation of this information. Traffic from one point to the other can be intercepted. Figure 5 shows eavesdropped traffic containing information sent in ASTERIX packet format. Initially the information is encrypted and cannot be understood, for the reason that Wireshark displays the information transmitted through the UDP(User datagram protocol) data transmission protocol. From the file it is possible to understand the IP from which the packets come and the IP to which they are destined. All addresses use different UDP ports for communication and are of different sizes.

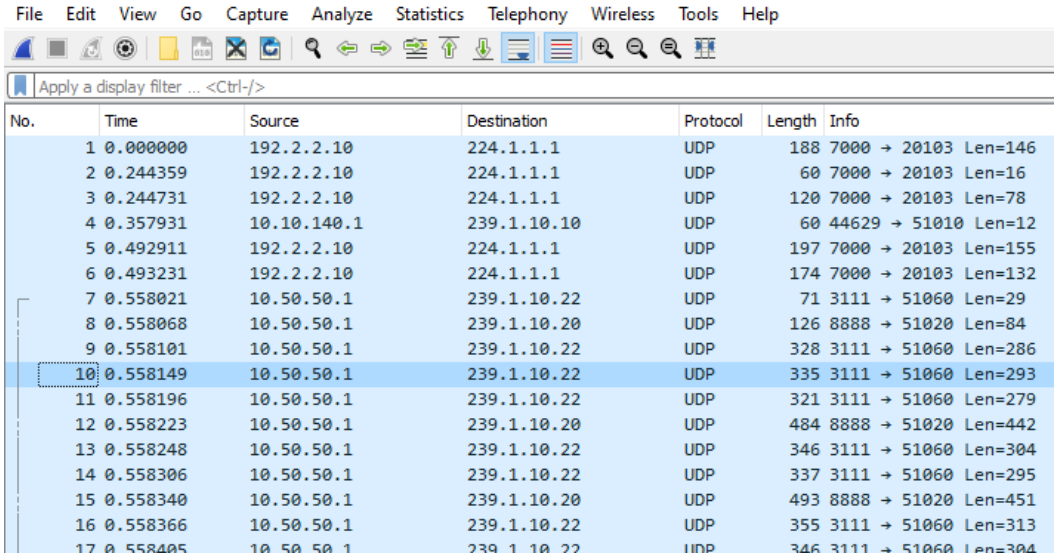

Figure 5. Eavesdropped traffic containing a message encoded using the ASTERIX protocol.

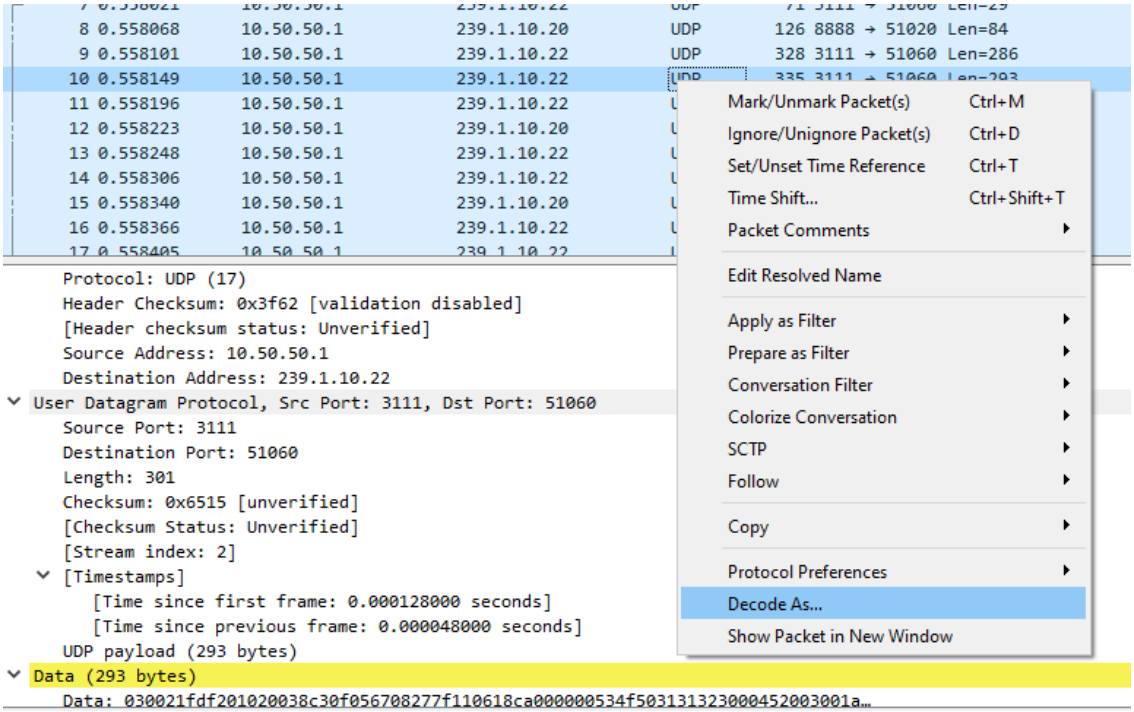

Figure 6. Selection of functionality for information decoding.

Figure 6 shows the ability to decode information from UDP to the ASTERIX protocol. The information contained in the tenth packet is completely unreadable. Using the decoding functionality of Wireshark, we choose to convert it to the ASTERIX protocol.

Figure 7 shows how Wireshark's decoding functionality converts UDP protocols into ASTERIX protocols.

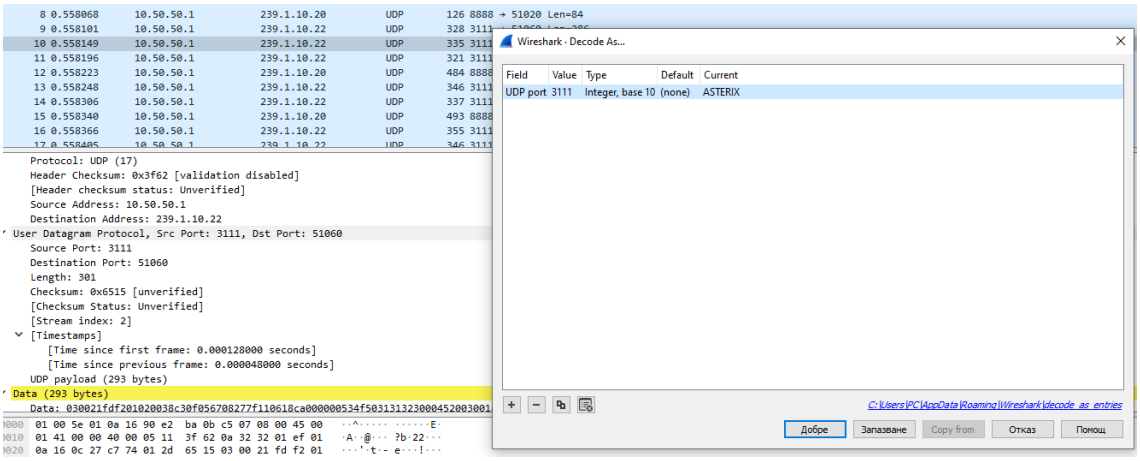

Figure 7. Decoding a UDP packet to the ASTERIX protocol.

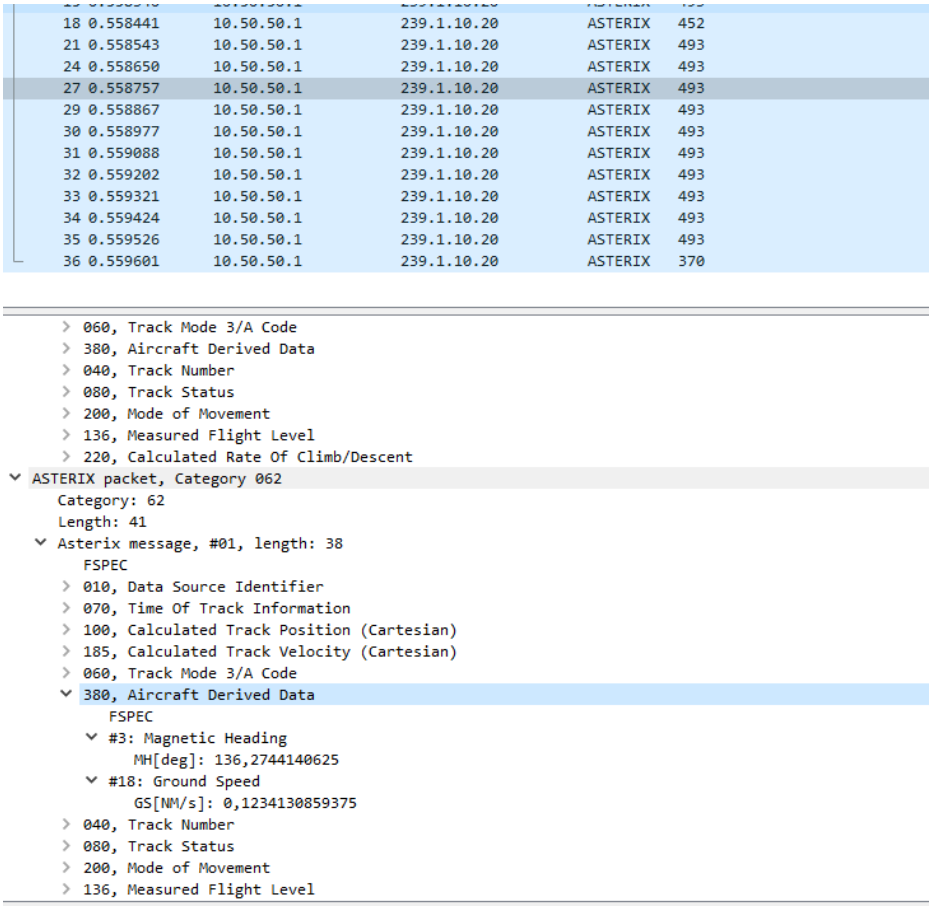

Figure 8. Detailed analysis of the ASTERIX package.

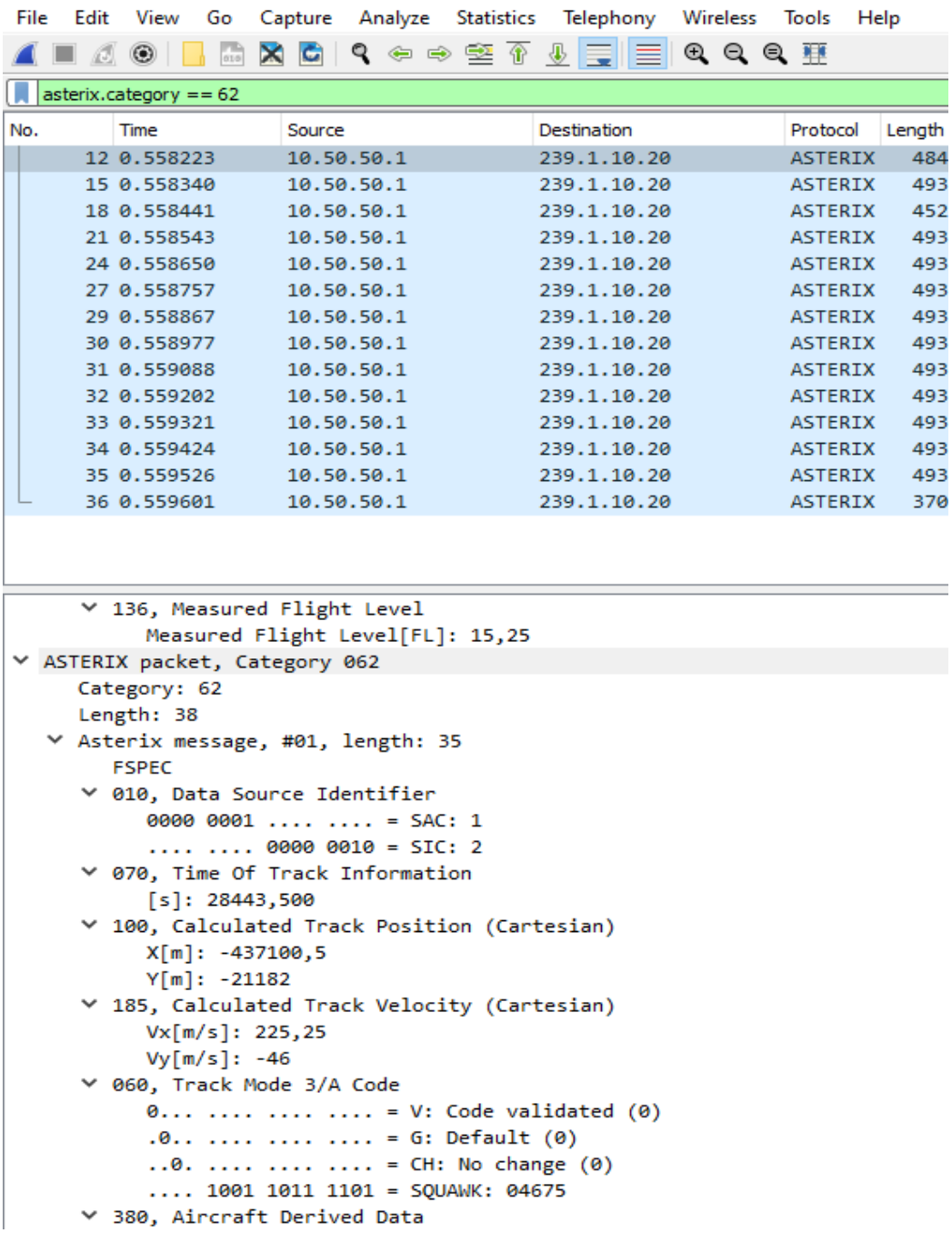

Figure 9. Filtering by category 062 of the ASTERIX protocol.

After decoding, the filtered information can be converted to ASTERIX format. The detail information that has been transmitted, can be seen to be analyzed, changed and resent in Figure 8. The data shown in Figure 9 has been filtered to show only from category 062 [10]. This makes it possible to filter the network packets only by packets that are for the aircraft system report.

Some of the problems do not come directly from attacks, but from problems in the software code. An example of this is the July 2020 bug in the UK airline TUI's software that confused the naming of "Miss" and "Ms" [11]. This gives a systematic error that identifies people who use the Miss designation as

children and sets their weight at times less than the actual weight. This is a prerequisite for confusing the calculations of aircraft load in flight and gives the possibility of fatal consequences. Examples of miscalculated aircraft loads ending in fatality include Cubana de Aviación's Field 972 in 2018 and a Fine Air Douglas DC-8 flight in 1997.

A report on the problem later revealed that this problem was first identified on July 10, 2020, when three passengers identified themselves as Miss and were registered as children in the program. Airline staff noticed the problem and resolved the issue manually. An unsuccessful attempt by the developers to fix the problem followed. 11 days later, the third, and last, TUI Airways flight BY-7226 with such a problem takes off with 167 passengers on board, 65 of them children. It was subsequently learned that there were in fact only 29 children. If this bug is discovered by hackers, it could turn into a zero-day attack and lead to a fatal end.

4. Recommendations and protections

Based on the analysis of attacks in Section 3, recommendations have been made to mitigate this type of malicious activity:

1. Eavesdropping using tools like WireShark can be avoided by using a VPN. The VPN would allow encryption of the data on both sides and so the data intercepted by Wireshark would be useless as the VPN encrypts the data and makes it impossible to decode.
2. Implementing an identification and authentication step after the date link layer of the ADS-B receiving protocol would prevent man in the middle attacks.
3. Optimize systems control. Provide reliable encryption, authorization, and authentication methods. Limit redundant access to highly sensitive computer configurations.
4. Cybersecurity training for teams working on and off airbases and airports. The goal of the training is to improve information security literacy to avoid insider attacks.
5. Prohibiting the use of any personal devices on airports and airbases. This is to protect against an already infected device that, when connected to the airport or airbase network, could spread or gain access to sensitive information.
6. The application of artificial intelligence would solve a large percentage of external and internal cyber threats. Using databases of various cyber threats already created by many different institutes, artificial intelligence could detect and block malware in the fastest and most optimal way. Artificial intelligence and machine learning can process large amounts of information in a short amount of time, making them favorites over conventional methods of defense. By building a neural network to analyze the performance of every suspicious file in systems, artificial intelligence avoids the weakness of "cloaking" some viruses, allowing them to be hidden from normal antivirus and firewalls. Another important advantage of artificial intelligence is that it can redirect resources to weak spots in a computer system when it is attacked. It will be possible to predict how and where defenses are most likely to be compromised, and a plan will be devised to redirect resources to address weaknesses. The use of artificial intelligence is critical to understanding the impact of various infosecurity programs and reporting relevant information to all stakeholders.

5. Conclusion

The continuous development of information technology and engineering has led to its integration into many of the systems used in aviation. This leads to the optimization of flight logistics and the handling of technical details. It also makes operators dependent on the help of modern software tools and leads to new threats. Over the last decade, we have seen a dramatic increase in cyber attacks, both on business areas as well as military and aviation infrastructures. Cyber attacks are fast, effective and cheap. With the

development of the Dark Web and cryptocurrencies, these attacks are becoming more accessible. All of this determines the danger of this type of malicious activity. The aviation industry is prone to this type of attack as they operate with billions of dollars of capital and at the cost of passenger safety. In order to be prepared for future cyber incidents, airport and airbase personnel should receive cyber security training. This would limit the impact of this type of attack. The implementation of artificial intelligence is of utmost importance for the development of cyber security of such key infrastructures.

References

1. “Aviation: Benefits Beyond Borders global report”, Aviation Benefits Beyond Borders, 2020

2. Wu Z., S. Tong, A. Guo, “Security issues in automatic dependent surveillance - broadcast (ads-b): a survey”, IEEE Access 2020, 8, 122147 - 122167

3. Mauro L., E. Piracci, G. Galati, “ADS-B vulnerability to low cost jammers: risk assessment and possible solutions”, 2014 Tyrrhenian International Workshop on Digital Communications - Enhanced Surveillance of Aircraft and Vehicles (TIWDC/ESAV), 2014

4. Gary K., J. P. Craiger, "Aviation cybersecurity: An overview", 2018

5. Andrew J. K., D. P. Shepard, J. A. Bhatti,T. E. Humphreys, “ Unmanned Aircraft Capture and Control Via GPS Spoofing ”, Special Issue: Special Issue on Low Altitude Flight of UAVs, Issue 4, 617-636

6. EUROCONTROL EATM-CERT Services, 2020, 12

7. Arjun K., “Hack attack leaves 1,400 airline passengers grounded”, CNBC, 2015

8. Sergiu G., “European Airport Systems Infected With Monero-Mining Malware”, Bleeping Computer, 2019

9. Wireshark, “Asterix”, https://wiki.wireshark.org/ASTERIX

10. European organisation for the safety of air navigation, “Eurocontrol standard document for surveillance data exchange. Part 9 : category 062. Transmission of system track data”, 2002

11. Thomas C., “Airline software super-bug: Flight loads miscalculated because women using 'Miss' were treated as children”,The Register, 2021