2022 14th International Conference on Cyber Conflict
Keep Moving
T. Jančárková, G. Visky, I. Winther (Eds.)
2022 © NATO CCDCOE Publications, Tallinn

Security and Privacy Issues of Satellite Communication in the Aviation Domain

Georg Baselt
ETH Zurich
Department of Computer Science
Zurich, Switzerland
gbaselt@student.ethz.ch

Martin Strohmeier
Cyber-Defence Campus
armasuisse Science + Technology
Thun, Switzerland
martin.strohmeier@armasuisse.ch

James Pavur
University of Oxford
Department of Computer Science
Oxford, United Kingdom
james.pavur@cs.ox.ac.uk

Vincent Lenders
Cyber-Defence Campus
armasuisse Science + Technology
Thun, Switzerland
vincent.lenders@armasuisse.ch

Ivan Martinovic
University of Oxford
Department of Computer Science
Oxford, United Kingdom
ivan.martinovic@cs.ox.ac.uk

Abstract: Modern aviation systems increasingly use satellite channels for data communication. However, many SATCOM providers do not offer encryption below the application layer by default, making their services vulnerable to eavesdroppers and creating security concerns. This research analyses such vulnerabilities specifically with regard to the aviation domain.

We show that even low-resourced attackers can exploit this lack of security. We capture a broad range of SATCOM transmissions in the Ku-Band frequencies using a TV Tuner Card and widely available low-budget equipment for under 400 US dollars. Over 370 GB of aviation-related satellite-downstream data from high-throughput satellites were analysed from a measurement site in Central Europe.

The results of this campaign reveal both security and privacy concerns across the whole spectrum of the industry. We identify unencrypted SATCOM usage comprising usage from in-flight entertainment systems to leaked private encrypted keys. Furthermore, we identified 328 specific aircraft broadcasting their live operations, including three government aircraft that actively blocked any information on their flights from air-traffic tracking sites.

This work concludes with recommendations for both satellite service providers and aviation stakeholders on how these issues could be solved by using encryption at different network layers.

Keywords: *aviation, satellite security, privacy, communication*

1. INTRODUCTION

The aviation industry is one of the world's largest and most important transportation businesses, carrying billions of passengers every year. The International Civil Aviation Organization ICAO estimated that in 2019 alone, a total of 4.5 billion passengers travelled by aircraft, an increase of almost 1.7 billion compared to just ten years earlier [1]. Their projections from 2019 foresaw a total increase to 10 billion passengers per year worldwide by the year 2040. Although this estimated rapid growth has slowed due to the COVID-19 pandemic, the trend remains clear.

A key technology enabling this growth is the usage of satellite communications (SATCOM). Satellite channels allow for fast message transfers in hard-to-reach areas such as oceans, where other communication methods cannot be used. Therefore, they offer reliable bandwidth and higher speeds for both entertainment and safety-critical systems compared to traditional air-to-ground links.

While SATCOM enables aircraft to be as connected as never before, it also introduces new risks and challenges. In particular, new concerns about privacy and data security have emerged in recent years [2]. Advancements in consumer technology saw the introduction of software-defined radios, which enabled its users to intercept aviation transmissions. This practically removed barriers to entry, as the necessary equipment to eavesdrop on aviation and satellite channels used to require specialist equipment [3].

This paper illustrates the prevalence of safety and privacy issues within the current satellite communication landscape in the aviation domain. We conduct the first study of aviation-related satellite transmissions using widely available low-cost equipment.

The contributions of this work are as follows:

i. We identify and map geostationary satellites that are used for aviation data link transmissions from a real-world dataset.
ii. We analyse aviation-related SATCOM transmissions and their impact on safety and privacy.
iii. We discuss the results and the implications of such vulnerabilities for the aviation domain and propose potential countermeasures.

The paper is structured as follows. First, background information on communication methods in the aviation industry as well as previous research efforts is given in Section 2. Section 3 explains the experimental setup and methods used to gather data, while Section 4 describes all relevant findings from the experiment. The results are then discussed in Section 5, before Section 6 concludes.

2. BACKGROUND

Communication plays a vital role in managing modern air traffic worldwide. A wide range of messages are sent from and to aircraft to ensure safe and efficient travel in the skies. While early communication systems provided simple voice communication channels from air to ground and vice versa, nowadays messaging services can send and receive automated information about optimal flight routes, positioning information, real-time weather reports and more. On top of the more complex air traffic control (ATC) messages, airlines have identified in-flight internet connectivity as a strong interest of a changing generation of customers. A report by Panasonic states that 'millennials become the largest air travel spending segment by 2025' [4]. According to the same report, '… one in three passengers are choosing airlines based on connectivity and quality of network service.' This development leads to aircraft sending and receiving more messages than ever before. The following chapter aims to provide a brief overview of current communication methods and their usage in the aviation domain.

A. Communication Methods in the Aviation Domain

There are three main categories of communication methods used in the aviation industry today. Figure 1 shows a simplified overview of these systems and their usage in a few selected applications – the Aircraft Communications, Addressing and

Reporting System (ACARS) and the Controller Pilot Data Link Communications (CPDLC) service.

1) Voice Communication

Today's standard method of air-to-ground communication is by voice broadcast over radio frequencies from 3 MHz to 300 MHz, known as VHF and HF. The development of this technology dates as far back as the 1920s and is still the backbone of modern air traffic control (ATC). VHF communication is used to manage densely populated airspaces, where their line-of-sight limited range plays no significant role. Voice communication over HF offers nearly worldwide coverage, even in polar or oceanic regions, but comes at the cost of the signal-to-noise ratio being dependent on atmospheric conditions, which makes it an unreliable choice for handling time-critical ATC messages [6]. As voice communication channels become increasingly congested in areas with high air traffic intensity, there are multiple avenues to shift ATC from voice to datalink channels.

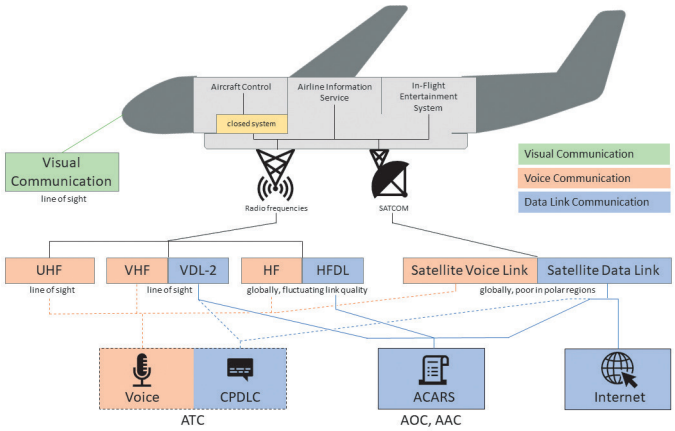
2) Datalink Communication

Datalink communication consists of exchanging digital messages between air and ground. The first system using data links was the Aircraft Communications, Addressing and Reporting System (ACARS) from 1978. It was initially developed to reduce the workload of radio control personnel and to automatically send messages about OOOI[1] events, which informed the receiver about the exact timestamps when the aircraft entered a new major flight phase. Nowadays, ACARS is used to transmit a wide range of clear-text messages to different aviation industry stakeholders, such as Aeronautical Operational Control (AOC) or Airline Administrative Control (AAC) messages to the ground base control of airlines [6].

Another datalink communication system is the Controller Pilot Data Link Communication (CPDLC) service. It serves as a supplementary ATC messaging channel to voice communication and allows its users to send preformatted ATC messages for non-time-critical requests, which significantly reduces the risk of communication errors. Like voice communication, datalink messages can be sent using radio frequencies or alternatively over a satellite connection.

1 Out of the gate, off the ground, on the ground, into the gate.

FIGURE 1: ABSTRACT VIEW OF COMMUNICATION METHODS USED WITHIN THE AVIATION INDUSTRY

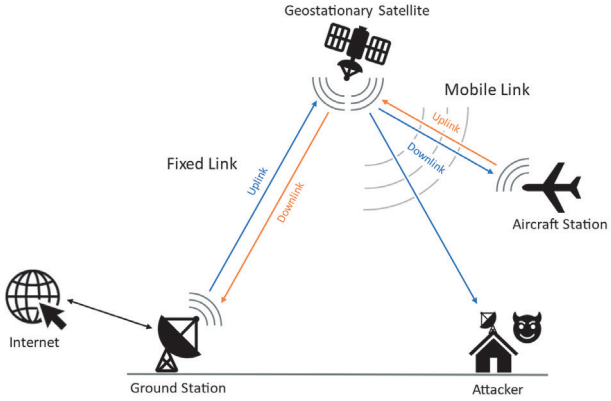


3) Satellite Communication (SATCOM)

For aircraft to use bidirectional SATCOM links, they must be equipped with an SDU (satellite data unit), an antenna and a high-power amplifier. These devices enable aircraft to send messages over radio frequencies via an uplink connection to a satellite, which then relays the received message stream from the aircraft to a ground station. SATCOM datalinks are a two-way communication system, as messages can also be sent from the ground station to the aircraft using the satellite as an intermediate step that broadcasts messages back to the aircraft. The system is depicted in Figure 2 for the case of geostationary (GEO) satellites, which we examine in the present work.

GEO downlink broadcasts can freely be recorded by everybody in the satellite coverage area with the right technical equipment. Messages sent in any other direction could potentially also be listened to, but this would require the eavesdropper to be near the satellite or ground station, as these beams tend to be directed towards their target and are narrower.

FIGURE 2: EAVESDROPPING MODEL ON SATELLITE DOWNLINK COMMUNICATION



Historically, the necessary equipment to receive satellite downlink broadcasts was expensive and difficult to acquire. This effectively acted as a protective barrier for ATC technologies, which have often not been developed with security in mind. ACARS, especially Plain-Old-ACARS, for example, is now used for far more than originally intended and has no default encryption scheme. This barrier-of-entry vanished when software-defined radios (SDR) and applications built on them became widely available in recent years. Attackers are now able to eavesdrop on unencrypted, aviation-related SATCOM feeds using relatively cheap and publicly available equipment.

B. Previous Research

More than a decade ago, Sampigethaya *et al*. first aimed to raise awareness regarding the transition towards fully interconnected flights, such as handling air traffic management over IP [5]. Recently, several works have examined concrete security and privacy issues both in non-satellite aviation datalinks and in satellite networks in different transport domains.

Smith *et al*. [6] use recordings of traditional radio frequencies and SATCOM feeds to illustrate the strong privacy concerns for passengers and crew. With regard to cyber security problems in aviation, research has greatly expanded over the past ten years, covering the full range of communication technologies used by different types of aircraft. For a full survey of these aspects, the reader is referred to [7]. The possible impact of cyber security attacks on safety in aviation has been studied in simulators, indicating the potential for severe disruption [8]. A survey by Strohmeier *et al*. [9], examines the missing awareness from stakeholders inside the aviation industry about such cyber security issues.

Bernsmed *et al*. [10] conducted a risk analysis on the security of future aviation-related SATCOM datalink services. They found severe security concerns in the studied services, where, in some cases, security issues were in direct conflict with safety requirements. The practicability to exploit such security and safety risks was shown by Santamarta in [11]. The authors illustrate the ability of an attacker 'to disrupt, intercept or modify non-safety communications such as InFlight Wi-Fi' as well as 'to attack crew and passengers' devices'. That the use of unencrypted air traffic control links is as insecure in space as it is on the ground has been discussed by the authors in [12]. Finally, a study similar to ours but for the maritime domain was conducted in [3]. The authors illustrate how the unencrypted nature of satellite communication impacts the security of ships around the globe.

To the best of our knowledge, there has been no study where possible security and privacy issues within general-purpose SATCOM data streams used by aircraft have been analysed.

3. METHODS

This section gives an overview of our approach and covers the methods used as well as the technical equipment, both hardware and software.

A. Experimental Design

The goal of our study is to capture aviation-related communication to analyse it for potential safety or privacy issues. Downlink SATCOM messages from geostationary satellites can be received using low-level equipment and a wide footprint area.

Finding such satellites was the first step. We use an exploratory approach, where all geostationary satellites providing coverage at the reception site were identified using an online database. With their coordinates known, the satellite dish was then aligned to receive transmissions from these satellites.

These beams were then scanned for transmissions within specific frequencies and encoding methods. Once a data stream featuring suitable encoding was found, a sample was recorded as a video transport stream file. These files were then analysed by searching for any ASCII encoded aviation-related strings in their byte-code representation.

B. Hardware Setup

Our study followed the setup used in [3] for analysing SATCOM in the maritime domain. The required hardware consists of a satellite dish, a satellite TV tuner card

and a computer connected to it. By using a TV Tuner Card over a software-defined radio, we are better able to keep up with real-time data due to the faster demodulation capabilities of the TV Tuner. It is assumed that an eavesdropper already has access to the latter, which brings the total equipment cost down to under 400 US dollars, as can be seen in Table I.

TABLE I: HARDWARE EQUIPMENT AND COSTS [3]

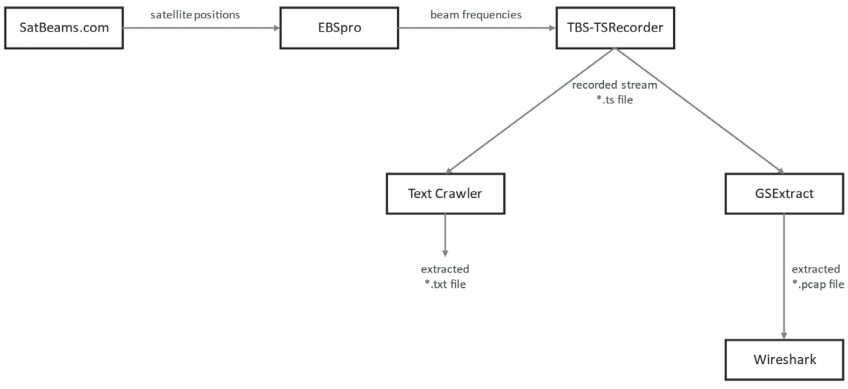
Item	Approximate Cost
TBS-6903 DVB-S2X PCI Card	$300
Selfsat H30D Satellite Dish	$88
3-meter Coaxial Cable	$5
Total	$393

The satellite dish model used for this project is widely commercially available and was combined with a professional-level digital satellite TV tuner card that supports all current digital video broadcasting standards over satellite (DVB-S). Located in Central Europe, with a size of only 517 × 277 × 58 mm, it can receive satellite feeds from all around Europe and parts of the Atlantic Ocean.

C. Software and Methodology

On top of the described hardware, we used open software tools and information in addition to our custom-developed software. Figure 3 provides an overview of the toolchain used for the study.

FIGURE 3: OUTLINE OF THE METHODOLOGY AND SOFTWARE USED TO CAPTURE SATCOM FEEDS



1) Obtaining Satellite Positions

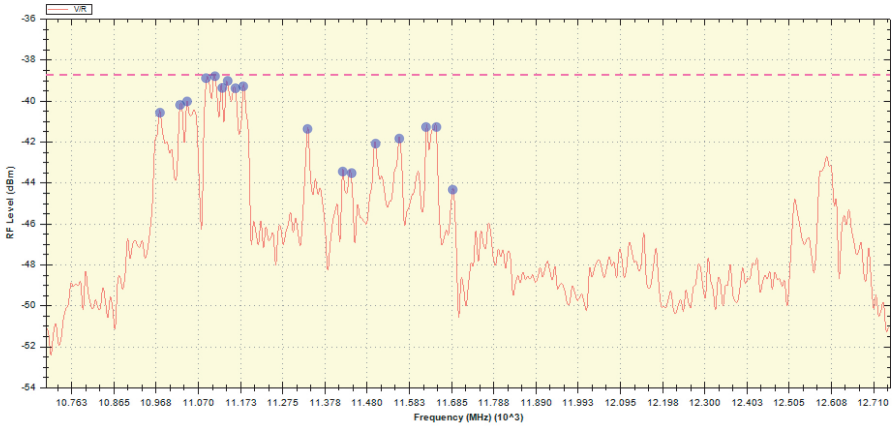
There are publicly available websites that host well-documented databases of satellites and their respective coverage areas. This project used satellite footprint data from the website SatBeams.[2] All geostationary satellites in positions from 30° West to 30° East, covering Central Europe and with beams in the Ku-Band (i.e. in the radio spectrum from 10700 MHz to 12750 MHz) were identified and used for further examination. The sixty-degree window was chosen because of the limitations of the satellite dish, as the signal of satellites farther away would be too weak to capture with the size of the dish used.

The Ku-Band frequencies were chosen, as previous research showed the presence of satellite downstream transmissions in this frequency range. [3]

2) Scanning for Frequencies

These satellite beams were scanned for data streams with a radio frequency using EBS-Pro.[3] We then identified possible data streams through spikes in the signal strength within these frequencies (Figure 4). This scan revealed the frequencies, symbol rates and other encoding meta-data of all satellite streams in this frequency range.

FIGURE 4: THE SIGNAL STRENGTH OF A SATELLITE BEAM IN THE KU-BAND FREQUENCIES. THE MARKED SPIKES REPRESENT POTENTIAL DATA STREAMS AND THE DASHED LINE BENCHMARKS, THE STRONGEST OBSERVED SIGNAL



3) Recording of Streams

Only a subset of all streams featuring some specific encoding schemes and protocols were used for this study. While it would be possible to scan for beams outside the Ku-Band range or with other encoding parameters with the described setup, this could

2 https://satbeams.com
3 https://ebspro.net

require different tools to analyse the recorded data, and therefore was not attempted. Nevertheless, it is reasonable to assume that the selected subset of streams is still representative of a wide range of SATCOM channels, as the chosen parameters are commonly used in practice.

The restrictions for the stream encoding parameters were:

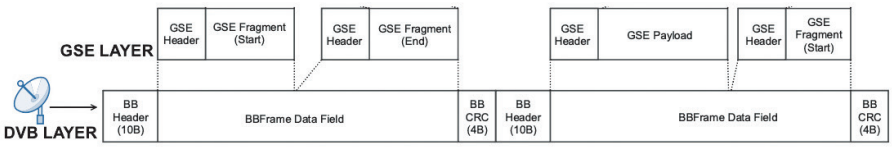
i. Only DVB-S2 streams with Adaptive Coding and Modulation (ACM) and Generic Stream Encapsulation (GSE) were considered.
ii. Only continuous data streams containing packets with MATYPE[4] headers of 42 00 or 43 00 were considered.
iii. Only streams using vertical polarization were considered.

From all the previously identified streams that met these conditions, an initial recording of 500 MB was saved. Later, additional, larger recordings of promising streams were conducted to obtain a larger sample.

4) Data Analysis

As the equipment comprised accessible, low-cost, consumer-grade hard- and software, the recordings can easily be fragmented or corrupted. To extract meaningful data from the lossy feeds, two different methods can be employed: one works on the DVB layer directly and the other targets the higher GSE layer (see Figure 5 for details on the protocol stack).

FIGURE 5: THE LOWER PROTOCOL STACK OF DVB-S COMMUNICATIONS, COMPRISING THE DVB AND THE GSE LAYER



a) GSExtract

For certain DVB-S2 Formats, the forensic tool GSExtract[5] is able to fully recover at least 40% [3] of the recorded GSE packets and convert them into more easily accessible IP traffic files (PCAP). This format can then be processed by Wireshark,[6] a tool for network protocol analysis. GSExtract loops through the recorded GSE-encapsulated files, searching for non-corrupted headers, and uses the information stored in the header to piece IP packets back together.

4 ETSI EN 302 307-1 V1.4.1 (2014-07)
5 https://github.com/ssloxford/gsextract
6 https://www.wireshark.org

b) Custom Text Crawler

The second method comprises a custom text crawler that extracts string segments consisting of alphabet letters, numerals, and other ASCII characters. This script matches strings in the recorded byte-files with keywords from a list and collects the coinciding strings in a text file. This helped to identify satellite streams that were used for aviation-related communication.

The list of keywords (55 in total) was constructed to contain aviation-related search terms such as ‘air’, ‘aero’, ‘flight’, as well as other communication-related words like ‘wifi’, ‘connect’, and ‘update’. This list was used to automatically obtain relevant satellite feeds, where deeper manual analysis could then be further conducted. This method is more universal than GSExtract and can be employed on all DVB-S2 streams.

D. Ethical and Legal Considerations

As the data collected in this experiment comes from real-world network traffic, all recordings were treated with special care to adhere to the current legal regulations of the local jurisdiction.

The recordings and all follow-up data used for the analysis were stored on a secured server and were fully removed once they were no longer needed. The content of all messages was treated as if it contained sensitive data, as no knowledge about the sensitivity of the data existed in advance. Where applicable, affected parties have been informed directly.

4. FINDINGS

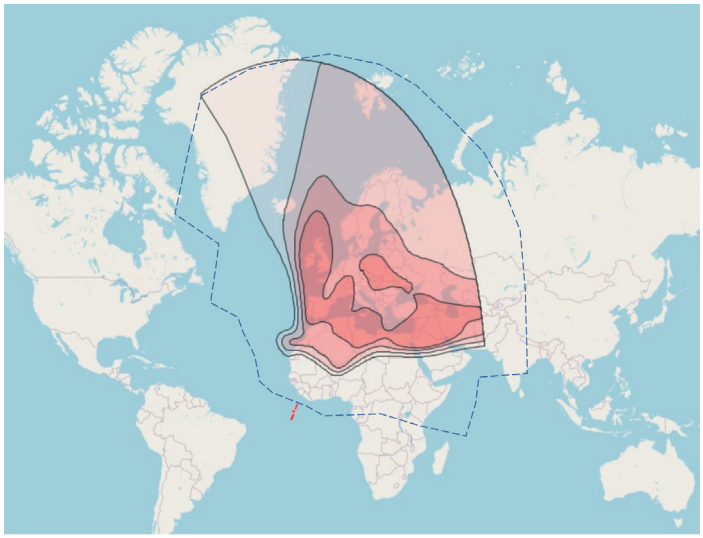
A total of 18 satellites were identified broadcasting in the Ku-Band frequencies as seen from our vantage point in Central Europe (Table II).

TABLE II: INFORMATION ON THE IDENTIFIED SATELLITES AND THEIR OBSERVED BEAMS. AS THEY ARE STATIONED IN GEOSTATIONARY ORBIT ABOVE THE EQUATOR, ONLY THE LONGITUDINAL COORDINATES ARE LISTED

Satellite Location	Satellite Name	Beam
1° West	Intelsat 10-02	Spot01
1° West	Thor 6	K2
1° West	Thor 5	T2
12° West	Eutelsat 12 West B	Europe
14° West	Express AM8	EuropeME
15° West	Telstar 12V	EuropeME
18° West	Intelsat 37e	Spot02
22° West	SES 4	EuropeME
24° West	Intelsat 905	Spot01
30° West	Hispasat 30W-6	EuropeNA
30° West	Hispasat 30W-5	Europe1E
5° East	Astra 4A	EuropeFSS
7° East	Eutelsat 7B	EuropeA
7° East	Eutelsat 7C	West
23° East	Astra 3B	PanEuropean
28° East	Astra 2E	Europe
28° East	Astra 2G	Europe
28° East	Astra 2F	Europe

We estimated their coverage footprint using the collected communications data, as shown by the dashed line in Figure 6. While each satellite footprint covers a different area, their complete collective footprint stretches around Europe and covers parts of the Atlantic Ocean, Northern Africa, and the Middle East.

FIGURE 6: THE COVERAGE FOOTPRINT OF THE MAIN AVIATION-RELATED SATELLITES OBSERVED IN OUR STUDY, REPRESENTED BY RED SHADES (LIGHTER SHADE ILLUSTRATING WEAKER SIGNALS). THE DASHED LINE INDICATES THE MAXIMUM OBSERVABLE AREA COVERED BY AT LEAST ONE SATELLITE LISTED IN TABLE II



Scanning these satellite positions for transmissions identified 34 frequencies, 26 from satellites positioned in the West and eight from satellites in the East. Over the course of 25 days in 2021, a sample file of 500 MB was recorded for each frequency.

The text crawler then identified five frequency recordings with potential aviation-related content. Since it was unknown from which satellite the signal of these beams was originating, a new set of longer recordings was conducted for all five constellations (Table III).

TABLE III: LIST OF DETAILED RECORDINGS OF BEAMS WITH AVIATION-RELATED CONTENT

Satellite Stream			Recording		
Location	**Frequency**	**Symbol Rate**	**Nr.**	**File Size**	**Duration**
12° West	11106 MHz	46657 KS/s	1	25.5 GB	73.5h
14° West	10984 MHz	51418 KS/s	2	67.0 GB	25.3h
12° West	11106 MHz	46657 KS/s	3	73.7 GB	20.5h
15° West	10985 MHz	51419 KS/s	4	87.7 GB	32.2h
15° West	11106 MHz	46657 KS/s	5	116.0 GB	28.3h

From inspecting the content of the newly recorded files, it turned out that the transmissions were sent from a high-throughput satellite, one of the 'leading satellites for mobile broadband maritime and aero services' [18]. Due to an incompatibility with the current version of GSExtract, the content of this feed was analysed exclusively using the text-crawling method. The red-shaded areas in Figure 6 show the footprint of these aviation-related satellite transmissions, with the lighter shades depicting weaker signals. In the following, we present first some results from an exploratory approach, followed by a more systematic analysis.

A. Exploratory Findings

Using an exploratory analysis, we present three main findings with regard to aviation-related communication on SATCOM streams from our study.

a) In-Flight Entertainment and Live Television

First, we observed unencrypted data originating from one of the world's leading service providers for in-flight entertainment (IFE) systems, which enables on-board live coverage of sports events, news broadcasts and other television programs with its global network of high-throughput satellites.

The messages contained technical information about the TV stream, such as encoding, aspect ratio, resolution, and audio language. It was also possible to obtain the port numbers of the channels and the private IPv4 address used for on-board transmission (Figure 7). During the period of the study, we observed 17 different TV channels, from international news to sports and entertainment.

FIGURE 7: MESSAGE PACKET CONTAINING INFORMATION ABOUT A CHANNEL PROVIDED BY A LEADING IFE SYSTEM

udioVideo","callSign":"NHK","image":"NHK","description":"Japanese-language chann
el designed to inform and entertain Japanese living and travelling outside Japan
. ","active":"1","name":W
"NHK World Premium","GndStreamAddress":"[redacted]","GndStreamPort":"[redacted]","v
ideo":{"id":"9","pid":"2048","resolution":"352x480","encoding":"h.264","aspect":
"16:9"},"audio":[{"id":"
12","pid":"8001","language":"jpn"}],"groups":[{"id":"1054"},{"id":"1001"},{"id":

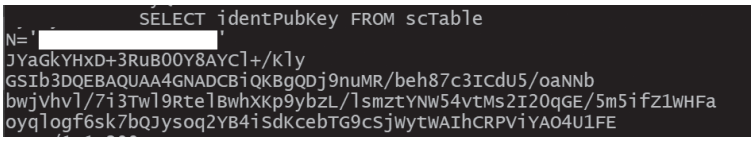
Knowing the IP addresses and ports from which these broadcasts are streamed may allow an attacker to hijack the television transmission by packet spoofing, imitating the stream's origin and replacing the content with their own. As an aside, as the captured messages did not indicate any form of encryption or authentication, this attack could become a real threat from someone inside the on-board network.

b) SQL Queries

Aside from data stemming from on-board entertainment systems, all five extensive recordings contained messages with two particularly noteworthy types of SQL

queries. The first one retrieves what looks like a public key from a database (Figure 8), opening up potential man-in-the-middle attack vectors, where public keys are replaced with malicious ones in transit. This makes it possible to decrypt and relay communication intended for the holder of the compromised public key.

FIGURE 8: OBSERVED SQL QUERY THAT RETRIEVES A PUBLIC KEY FROM A DATABASE



A second regularly observed and potentially vulnerable query inserts a commit into a database (Figure 9). Aside from a timestamp indicating the entry time of the log, different IDs and a 16-digit smart-card serial number are logged into the database. Smart cards can come in different shapes and are used for a wide range of purposes, from access control or authentication to financial transactions with a credit card. Having these queries sent openly and unauthenticated introduces, for example, the risk of replay attacks, where an attacker could capture the messages and send them again, possibly altering their content, such as the timestamp in the process.

FIGURE 9: EXAMPLE QUERY LOG COMMISSIONING SMART-CARD ENTRIES WITH TIMESTAMPS AND IDS

c) RSA Encryption Keys

Finally, the analysed transmissions contained large parts of private RSA keys in the PKCS#1 standard[7] (Figure 10). While the keys were not necessarily complete (due to lossy transmissions), RSA private keys should naturally never be exposed – even in part – due to their sensitive nature. The holder of a compromised private key should revoke and replace it immediately, as it opens up trivial attacks on the confidentiality and authenticity of any communication encrypted or signed with this private key.

Along with the private keys, the feeds also contained much shorter RSA public keys, which were complete and intact. This may pose a problem in specific man-in-the-middle circumstances, as discussed in the previous section.

7 https://datatracker.ietf.org/doc/html/rfc8017

FIGURE 10: AN INCOMPLETE (AND REDACTED) RSA PRIVATE KEY FOUND IN THE TRANSMISSIONS

B. Systematic Analysis of Aircraft and Stakeholders

We now analyse the type and owners of the aircraft seen during the study. In total, we could identify 328 different aircraft across 22 operators based on their tail numbers (see Table IV). These numbers were part of a message type captured in the recordings. Tail numbers are sufficient to identify an aircraft in conjunction with freely available online databases that reveal the aircraft type, its carrier airline, ICAO hex-codes and operator history [2].

TABLE IV: OVERVIEW OF AIRCRAFT IDENTIFIED BY THEIR BROADCASTED TAIL NUMBER

# of Aircraft	Operators	Registration Prefix	Registration Country
1	Japan – Air Self Defence Forces	-	Japan
11	Singapore Airlines	9V	Singapore
73	Emirates, Etihad Airways	T2	UAE
11	China Eastern Airlines, Air China, Cathay Pacific	B	China
37	Lufthansa	D	Germany
3	Iberia, Air Europe	EC	Spain
1	Alitalia	EI	Ireland
9	Air France, Aeroflot	F	France
7	British Airways, Virgin Atlantic	G	UK
2	Swiss	HB	Switzerland
2	Japan Airlines	JA	Japan
82	United Airlines, American Airlines, Aeromexico	N	USA
18	KLM	PH	Netherlands

3	Middle East Airlines	T7	San Marino
68	Turkish Airlines	TC	Turkey
328 aircraft	**22 airlines**		

Examples include aircraft used exclusively by the Japanese Prime Minister or members of the Imperial family for international travel (a Boeing 777-300ER). At the time, it was flying back from the 2021 G7 summit, which took place in Cornwall, UK, from 11 to 13 June.

Other notable aircraft identified were an Airbus A330-243 Prestige belonging to the Turkish Government and a Boeing 737-800 BBJ2 used for presidential flights of the United Arab Emirates. All three aircraft are blocked on flight tracking sites such as Flightradar24,[8] indicating a desire for privacy by their operators. As the captured messages circumvent these blocks by revealing concrete flight activity, we can see that even the most sensitive stakeholders can be affected by the lack of security on SATCOM links.

Our deeper analysis indicates that most aircraft using SATCOM are modern, wide-body aircraft belonging to major national flag carriers. This intuitively makes sense, as these airlines are generally more prone to invest in SATCOM connectivity and offer access to advanced entertainment systems, such as on-board Wi-Fi or live television, than low-cost carriers. The aircraft types found in the recordings also support this, as the benefit of extensive entertainment systems is assumed to be far greater on wide-body aircraft that cover long distances than on smaller, short-haul ones.

5. DISCUSSION

We now discuss our findings from the study. Table V presents an overview of the different issues found in our study and their potential impact on safety and security for passengers, crew, and operators.

8 https://www.flightradar24.com

TABLE V: OVERVIEW OF OBSERVED SATCOM ISSUES AND THEIR IMPACT ON SAFETY AND PRIVACY, ALONG WITH POTENTIAL ATTACK SCENARIOS EXPLOITING THE VULNERABILITY

Discovered Issue	Safety Impact	Privacy Impact	Attack Scenario
Wi-Fi Login Sites Visible	None	Potential for Strong Impact	Website Phishing
IFE system vulnerable	Potential for medium impact	None	Content spoofing
RSA private key messages	Impact unknown	Impact unknown	Message decryption
SQL queries visible	Impact unknown	Impact unknown	Replay attack
Tail numbers visible	Minor impact	Minor impact	Flight-path tracking

A. Communication Content Types

Our results show that widely used IFE and on-board Wi-Fi systems make use of unencrypted SATCOM channels for data transmission, allowing access to non-end-to-end-encrypted (E2EE) communication. On a cautiously positive note, and different to the maritime domain studied in [3], no email messages containing personal information from passengers were found during our time-limited study. A potential reason for this could be the use of E2EE by the observed systems. However, based on the recent literature, many non-E2EE systems are still in use, and examples may yet be found if the duration and scope of the study were extended.

As our study indicates, the use of insecure SATCOM systems on aircraft goes far beyond these passenger-oriented services. Traces of SQL queries and commits concerning public key and smart-card infrastructure are clear giveaways of crew- and business-related usage and several potential attack vectors.

As smart cards can be used for a large variety of tasks, it becomes more challenging to narrow down the purpose of the cards observed in our particular case. However, it seems reasonable to infer that the logs are used in the context of an employee time management system.

Other communication was not as readily identifiable using the applied methodology. However, we can speculate that observed XML files containing additional information about the carrier airline and a version number are likely part of the ‘Aircraft Earth Station (AES)’ management. AES comprises the setup and the billing of the SATCOM provider, providing a potentially crucial entry point for impersonation attacks.

B. Privacy Implications and Safety Concerns

In this part, the safety and privacy impacts of the findings are put into perspective with the likelihood of an attack exploiting these issues.

Starting with the general observation that the studied SATCOM channels do not deploy default encryption, simple eavesdropping attacks may result in a substantial breach of privacy. Although no emails or other personal messages were found during the present study, passengers of an airline offering unencrypted on-board internet access via a satellite connection are likely to leak private information over time. This may, for example, happen to unsuspecting users downloading their emails in clear text from an unsecured mail-server using POP3, as shown previously in the maritime context [3]. Artefacts in related studies also revealed mobile phone traffic originating from aircraft. [13]

The ability to track aircraft based on their SATCOM connections provides a potential operational security risk, as outlined in detail in previous literature (e.g. [2]). While not a concern for most commercial airlines, as their flight paths are well known and easily accessible, some of the identified aircraft actively hide their whereabouts from the public. All three observed government airplanes were either fully or partly blocked on public tracking sites, underlining their individual desire for privacy.

Aside from potential privacy concerns for crew and passengers, our study did not directly indicate message content, which could pose a direct risk for the safety of an aircraft. In particular, no connection to the safety-critical aircraft control domain was observed, which would make it possible to tamper with flight control systems.

However, the transmissions directed at the in-flight entertainment system could still have a direct impact on on-board safety. As previously described, message content for live television services contained information about which ports and local IP addresses were used to stream content to seat monitors or private devices. An attacker on board the aircraft and connected to the local network could try to perform an IP spoofing attack, imitating the stream origin, and replacing the television transmission with their own. Depending on the content of this new stream, this could lead to disinformation or unrest among the passengers, an attack vector suggested previously by Ruben Santamarta of IOActive [14].

Another potential safety compromising attack could make use of the clear-text database accesses. While the observed SQL queries do not seem to contain content concerning safety or privacy, the database itself could become the target of a directed attack. A malicious adversary could try to access the entire content stored in the database, which might result in a severe leak of private information. Alternatively, he could

carry out a replay attack of already seen queries or forge completely new queries. Although the exact purpose of the database and the logging queries are not clear, it is more than reasonable to assume that such interference would strongly impact any system working with it.

The last finding with the potential to affect safety or privacy involves transmitted RSA private keys. As it was not possible to identify why or to whom they were sent, it is difficult to measure their direct impact. Nonetheless, the application or protocol that sends these messages is strongly violating any good practice in information security, and further investigations may lead to identifying further vulnerabilities.

C. Countermeasures

Finally, we review possible solutions to the issues discussed with respect to the specific environment of the aviation industry. There are two principal levels at which improvements to the safety and privacy of satellite communication can be applied.

The first option involves the satellite service providers, who are in the best position to improve the confidentiality of any data sent over their satellite network. As previous studies in other domains have shown, the industry-standard level of protecting satellite communication is insufficient and should be strongly reconsidered [3]. In response to this non-satisfactory situation, the academic research community has recently studied protocols and methods for provable secure satellite communication systems (e.g. [15], [16]). One of these promising approaches is QPEP, a protocol built on top of the QUIC standard, providing the performance benefits of industry-standard Performance Enhancing Proxies (PEPs) while offering the security of end-to-end message encryption at the same time [17].

As satellite service providers might not be inclined or able to make these changes to the data security of their satellite network traffic quickly (e.g. due to operational or financial reasons), another approach could see those manufacturers responsible for the development of IFE and on-board Wi-Fi systems improve their security practices. In addition to reviewing the use of SATCOM for sensitive content, this could involve the utilization of higher layer end-to-end encryption for all applications available on board.

However, with the aviation industry's historically strong focus on the safety of systems with multiple redundant layers, providing security guarantees on this level could be very challenging. A research project by Bernsmed *et al.* [10] on this topic advocates for a system where both sides provide certain security guarantees, stating that: 'SATCOM datalink systems must enable integrity protection and data-origin authentication of the

datalink applications, whereas confidentiality and non-repudiation protection should be implemented on an application-by-application basis.' [10]

Aside from any technical countermeasures, raising awareness of the issues with SATCOM usage in the aviation domain will be pivotal for the successful implementation of safe and secure datalink communication systems in the future.

D. Limitations

As our study was carried out using low-end commercial off-the-shelf equipment accessible to unsophisticated threat actors, some natural limitations exist. While the quality of the recorded files was sufficient to explore aviation-related content, the transmitted data was often cut short or corrupted due to lossy connections during the recording. It also needs to be stated that this experimental setup could only intercept satellite downlink messages sent towards an aircraft. To analyse different satellite streams, the receiver station would need to be positioned differently – in proximity to a ground station.

E. Further Research

The insights gained from this project represent interesting new options for future research.

One such topic could be the identified possibility of spoofing attacks on the in-flight entertainment system. Follow-up research could investigate the feasibility of such an attack, which might lead to a general study on the safety and security of on-board wireless networks.

Other studies could focus on the origin of the observed messages – for example, looking into which protocols or algorithms sent the RSA keys or the aircraft tail numbers. For these projects, it would prove beneficial to adapt the GSExtract tool to handle more relevant types of data recordings and collect detailed statistics on the type of network traffic similar to [3].

Finally, as this project only focused on satellite downstream transmissions, an interesting new approach would certainly be to intercept satellite upstream messages sent by an aircraft towards a satellite. Even though this requires an entirely different setup, the results would provide new insights into aircraft-to-ground satellite communication.

6. SUMMARY AND CONCLUSION

The goal of this work was to find and analyse safety and privacy-related issues of satellite communications inside the aviation domain. The findings from the conducted experiment and the subsequent analysis of the recorded files prove the existence of such problems and show that an eavesdropper can intercept SATCOM messages using widely available low-budget equipment. The results included streaming data related to the in-flight entertainment system of modern aircraft, as well as different messages containing SQL queries, on-board Wi-Fi addresses and RSA private keys.

With the present study, we want to raise awareness regarding the fact that the current state of play may compromise the confidentiality and integrity of sensitive aviation data, as attackers may try to exploit them. We believe that stakeholders inside the aviation industry need to adapt to the new threat environment of cheap and easily accessible satellite communications. As the future of air traffic management is going to rely heavily on SATCOM-based communication, security concerns need to be addressed with the same priority as safety is currently. As shown by previous works, the interconnected air traffic management systems of the future cannot be deemed safe while their security is not guaranteed. [8]

In addition to presenting technical approaches to secure satellite communication channels, this research has also illustrated the importance of raising public awareness of this topic, as all stakeholders travelling on SATCOM-connected aircraft can also be affected without their knowledge.

REFERENCES

[1] ICAO, 'The World of Air Transport in 2019', 2019. Accessed: Aug. 13, 2021. [Online]. Available: https://www.icao.int/annual-report-2019/Pages/the-world-of-air-transport-in-2019.aspx

[2] M. Strohmeier, D. Moser, V. Lenders, M. Smith, M. Schäfer, and I. Martinovic, 'Utilizing Air Traffic Communications for OSINT on State and Government Aircraft', in *Cyber Conflict (CyCon) 2018 10th International Conference*, Tallinn, Estonia, 2018.

[3] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, 'A Tale of Sea and Sky: On the Security of Maritime VSAT Communications', in *2020 IEEE Symposium on Security and Privacy (S&P)*, 2020.

[4] Panasonic Avionics Corporation, 'Why Passengers Are Demanding Live Television', 2020. Accessed: Aug. 3, 2021. [Online]. Available: https://www.panasonic.aero/our-offerings/solutions/theatre/live-television/#download-book

[5] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, and C. Royalty, 'Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond', in *Proceedings of the IEEE*, Nov. 2011, vol. 99, pp. 2040–2055.

[6] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, 'Undermining Privacy in the Aircraft Communications Addressing and Reporting System (ACARS)', in *Proceedings on Privacy Enhancing Technologies*, Jun. 2018, vol. 2018, pp. 105–122.

[7] M. Strohmeier, I. Martinovic, and V. Lenders, 'Securing the air–ground link in aviation', in *The Security of Critical Infrastructures*. Cham, Switzerland: Springer, 2020, pp. 131–154.

[8] M. Smith, M. Strohmeier, J. Harman, V. Lenders, and I. Martinovic, 'A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems', in *The Network and Distributed System Security Symposium* (NDSS), 2020.
[9] M. Strohmeier, A. K. Niedbala, M. Schäfer, V. Lenders, and I. Martinovic, 'Surveying Aviation Professionals on the Security of the Air Traffic Control System', in *International Workshop on Cyber Security for Intelligent Transportation Systems*, 2018, pp. 135–152.
[10] K. Bernsmed, C. Frøystad, P. H. Meland, and T. A. Myrvoll, 'Security requirements for SATCOM datalink systems for future air traffic management', in *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*, 2017, pp. 1–10.
[11] R. Santamarta, 'Last Call for SATCOM Security', IOActive, 2018. [Online]. Available: https://ioactive.com/wp-content/uploads/2018/08/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf
[12] M. Strohmeier, D. Moser, M. Schäfer, V. Lenders, and I. Martinovic, 'On the Applicability of Satellite-Based Air Traffic Control Communication for Security', *IEEE Communications Magazine*, vol. 57, no. 9, pp. 79–85, 2019.
[13] J. Pavur, 'Whispers Among the Stars', in *DEF CON "Whispers Among the Stars: A Practical Look at Perpetrating (and Preventing) Satellite Eavesdropping Attacks." In Conference briefing. Conference briefing. Black Hat USA*. Las Vegas, NV, Aug, vol. 5. 2020 Safe Mode, 2020.
[14] R. Santamarta, 'In Flight Hacking System', IOActive, Dec. 12, 2016. [Online]. Available: https://ioactive.com/in-flight-hacking-system/
[15] K. Guo, K. An, B. Zhang, Y. Huang, X. Tang, G. Zheng, and T. A. Tsiftsis, 'Physical Layer Security for Multiuser Satellite Communication Systems with Threshold-Based Scheduling Scheme', *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 5129–5141, 2020.
[16] M. Qi and J. Chen, 'An enhanced authentication with key agreement scheme for satellite communication systems', *International Journal of Satellite Communications and Networking*, vol. 36, pp. 296–304, 2018.
[17] J. Pavur, M. Strohmeier, V. Lenders, and I. Martinovic, 'QPEP: An Actionable Approach to Secure and Performant Broadband from Geostationary Orbit', The Network and Distributed System Security Symposium (NDSS), 2021.
[18] Telesat, 'Telstar 12 VANTAGE', Dec. 2020. [Online]. Available: https://www.telesat.com/wp-content/uploads/2020/12/Telstar-12-VANTAGE.pdf