Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS

Matthew Smith[1], Daniel Moser[2], Martin Strohmeier[1], Vincent Lenders[3], and Ivan Martinovic[1]

[1] Department of Computer Science, University of Oxford, United Kingdom
`first.last@cs.ox.ac.uk`
[2] Department of Computer Science, ETH Zürich, Switzerland
`first.last@inf.ethz.ch`
[3] armasuisse, Switzerland `first.last@armasuisse.ch`

Abstract. Recent research has shown that a number of existing wireless avionic systems lack encryption and are thus vulnerable to eavesdropping and message injection attacks. The Aircraft Communications Addressing and Reporting System (ACARS) is no exception to this rule with 99% of the traffic being sent in plaintext. However, a small portion of the traffic coming mainly from privately-owned and government aircraft is encrypted, indicating a stronger requirement for security and privacy by those users. In this paper, we take a closer look at this protected communication and analyze the cryptographic solution being used. Our results show that the cipher used for this encryption is a mono-alphabetic substitution cipher, broken with little effort. We assess the impact on privacy and security to its unassuming users by characterizing months of real-world data, decrypted by breaking the cipher and recovering the keys. Our results show that the decrypted data leaks privacy sensitive information including existence, intent and status of aircraft owners.

1 Introduction

Aviation is undergoing a period of modernization which is expected to last until at least 2030, with the International Civil Aviation Organization (ICAO) aiming to reduce emissions, increase safety and improve efficiency of air transport [11]. This program seeks to replace ageing avionic systems with newer solutions, a significant section of which revolves around avionic data links.

The main data communications system in current use is the Aircraft Communications Addressing and Reporting System (ACARS). A general purpose system, it has become the standard to transfer a wide range of information; for example, it is often used by crews to request permission from air traffic control (ATC) to fly a particular part of their route. Although ACARS will be replaced at some point in the future, this migration is unlikely to be completed within the next 20 years [11]. In the meantime, the vast majority of commercial aircraft and business jets must use ACARS for their data link needs.

Like many current wireless air traffic communication technologies, ACARS was designed several decades ago when security was not considered a main objective. Consequently, it did not include any form of encryption during its original standardization. Due to the technological advantage that aviation held over most potential threat agents, this fact did not raise significant attention over two decades. In recent years, however, cheap software defined radios (SDRs) have changed the threat landscape [21]. Using low-cost hardware and software downloadable from the internet, the capability to eavesdrop on ACARS has become commonplace.

The impact of this changing threat on security and privacy of the data link are manifold: among other possibilities, adversaries can track sensitive flight movements of private, business or government aircraft; confidential information such as financial or health information can be read and compromised; and potentially safety-related data such as engine and maintenance reports can be modified.

As users of ACARS became aware of its practical insecurity and demanded improvements to the confidentiality of their data, several cryptographic solutions were developed to provide a short-term fix but then these became long-term solutions. Only one of these solutions, a proprietary approach, is extensively used. Unfortunately, it has many serious design flaws — the most serious being that it is a mono-alphabetic substitution cipher — which negate any potential security and privacy gain. Indeed, as we argue in this work, this type of solution provides a false sense of security for ACARS users and consequently does more harm for their reasonable expectations of privacy than no solution at all.

Contributions

In this paper, we present our findings on a specific security vulnerability of the aviation data link ACARS. Our contributions are as follows:

- We show that the current most commonly used security solution for ACARS is highly insecure and can be broken on the fly. We analyze the shortcomings of the cipher used in this solution and its implementation.
- We quantify the impact on different aviation stakeholders and users. We analyze the extent of the privacy and security breach to its unassuming users, in particular owners of private and business jets, and government aircraft.
- From this case study, we provide lessons for the development of security solutions for existing legacy technologies, particular in slow-moving, safety-focused critical infrastructure sectors.

The remainder of the paper is structured as follows: We consider privacy aspects in aviation in Section 2 and our threat model in Section 3. Section 4 describes the workings of ACARS before we illustrate steps taken to break the cipher in question in Section 5. The impact of the weakness of the cipher is explained in Section 6. In Section 7, we discuss the lessons learned from this case and make recommendations for the future. Section 8 covers the related work, Section 9 covers legal and ethical considerations, before Section 10 concludes.

2 Privacy in Aviation

This section discusses a widely used mechanism with which an aircraft owner can protect their privacy, and the privacy expectations of private aircraft.

2.1 Blocked and Hidden Aircraft

Whilst no provision exists to restrict the sharing of flight information relating to commercial aircraft, it does for smaller, private aircraft. Schemes such as the Federal Aviation Administration's (FAA) Aircraft Situation Display to Industry (ASDI) register allow aircraft owners to restrict the tracking of their aircraft [9]. Some years ago, the scheme changed requiring that for a block to be implemented, a "valid security concern" must be demonstrated [6]. This included a "verifiable threat" against an individual, company or area, illustrating the severe privacy requirements of such entities. Since then, the scheme has been once more relaxed to allow any non-commercial aircraft owner to register a block [8]; even so, we claim that any aircraft owner is making a clear effort to protect their privacy in requesting a block.

ASDI is a data feed produced by the FAA and offered to registrants such as flight tracking websites. The FAA offers two levels of block for this feed — either at the FAA dissemination level, or at the industry level [7]. With the former, information about the aircraft is not included in the ASDI feed at all, whereas for the latter, the requirement to not share the data lies on the registrant. The requesting aircraft owner can choose which level of block to use, however if none is stated, the FAA defaults to the FAA-level block.

In practice, an ASDI-blocked aircraft will display either no information at all, or only rudimentary information such as the registration, on flight tracking websites. If an aircraft uses the FAA-level ASDI block then information about it can usually only be sourced from third-party databases such as Airframes.org (see Section 4.5 for more details). If an aircraft does not appear even in such third-party sources, we consider them 'unknown'.

Blocking aircraft in this way is particularly relevant as air traffic management is modernized. Most continents are in the process of mandating that new surveillance technologies be fitted to aircraft flying in classified airspace. These will automatically report flight data, thus meaning that schemes such as ASDI blocks will become a key factor in private aircraft user privacy.

2.2 Privacy Expectations

We consider these aircraft which make an effort to hide their activities to be privacy sensitive. More specifically, we consider them sensitive with respect to existence, intention, and status. These three categories are defined as follows:

- **Existence**: Observing an aircraft in the collection range. Simply receiving a message from an aircraft is enough to reveal its existence.

- **Intention**: ACARS messages that reveal what the aircraft will do in the future of its flight; for example, when and where it will land.
- **Status**: Information which describes the current activities of the aircraft. This includes current location, its flight origin, or the flight altitude.

By restricting appearance on flight tracking websites, users of these aircraft make a concerted effort to hide information belonging to each of these categories. Thus, ACARS messages revealing such information can be considered a breach of these privacy expectations.

3 Threat Model

As the basis of our model, we consider an honest-but-curious attacker who is passive with respect to the medium but actively decrypts messages: they collect ACARS messages and aim to break the cipher and decrypt messages that use it.

An attacker of this capability could achieve their aims for a relatively low financial outlay. A low-cost computer such as a Raspberry Pi is sufficient to run the collection, connected to a $10 RTL-SDR stick. Using freely available, open source software and a standard VHF airband antenna available for under $150, an attacker will be able to collect ACARS messages from aircraft. The ease-of-use and availability of SDRs has in turn created an active community which produces a range of free and open-source tools. Avionic communications are no exception, with several tools available to decode ACARS messages, for example. This has brought previously hard-to-access avionic communications into the domain of relatively low-skilled users.

We consider a typical attacker to operate from a single location with the aforementioned equipment, collecting and attempting to decipher messages over a number of months. A more capable attacker would be able to deploy multiple collection units across a larger geographic area in order to increase the message collection rate and the number of unique aircraft observed. As demonstrated below, this will increase the rate at which the analyzed cipher can be broken.

Intention also affects the magnitude of threat — an honest-but-curious attacker is likely to be small scale, while threat agents with specific motives could afford a larger-scale collection. Indeed, tracking aircraft movements as part of insider trading has been used in the past (e.g., [10]), which will require a wider collection network to increase the chance of sightings.

4 Aircraft Communications Addressing and Reporting System

In this section, we describe ACARS, its message structure and methods of transmission, the use cases in aviation, and finally, the existing security mechanisms.

Table 1: Comparison of ACARS delivery sub-networks

Mode	**Coverage**	**Frequency**	**Link Speed**
HF	Worldwide	2-30 MHz[4]	Up to 5.4 kbps[5]
'Plain Old' VHF	Continental, over land	∼131 MHz	∼2.4 kbps
VHF Data Link mode 2	Continental, over land, limited deployment	∼136 MHz	∼30 kbps
SATCOM	Worldwide, except polar regions	L-Band (1-2 GHz) uplink C-Band (6-8 GHz) downlink	Either 10kbps or up to ∼400kpbs[6]

4.1 ACARS at the Physical Level

ACARS is widely utilized around the world as an avionic communications system. Deployed in 1978, it provides support for airlines and ATC to communicate with the vast majority of commercial aircraft [13]. For example, airlines transfer flight plans via ACARS, while ATC issues clearances for particular routes.

ACARS has three delivery methods — High Frequency (HF), satellite (SATCOM) and Very High Frequency (VHF) [14]. VHF is further subdivided into 'Plain Old' ACARS (POA) and VHF Data Link Mode 2 (VDLm2) ACARS, the latter using a general purpose aviation data link. SATCOM ACARS is offered via the Iridium and Inmarsat satellite constellations, each with slightly different options and service levels. The key properties are summarized in Table 1.

A high-level diagram of VHF ACARS is shown in Fig. 1a, with SATCOM ACARS depicted in Figure 1b. Messages are transmitted between an aircraft and ground stations managed by service providers. Generally, service providers handle the infrastructure apart from the aircraft and endpoints. For ACARS, endpoints can either be ATC in order to manage air traffic, or airline administration who use ACARS for fleet operational purposes.

4.2 ACARS Messages

All versions of ACARS have the same message structure built around a free text element which forms the largest part of the message (see Fig. 2). Although the system character set is ASCII, Aeronautical Radio Inc. (ARINC) standard 618 notes that most parts of the network are only compatible with a reduced ASCII set [2]. However, to guarantee all parts of the network can handle the message content, the even further reduced Baudot character set would need to be used, effectively limiting the set to `A-Z`, `0-9`, `,-./`, and some control characters.

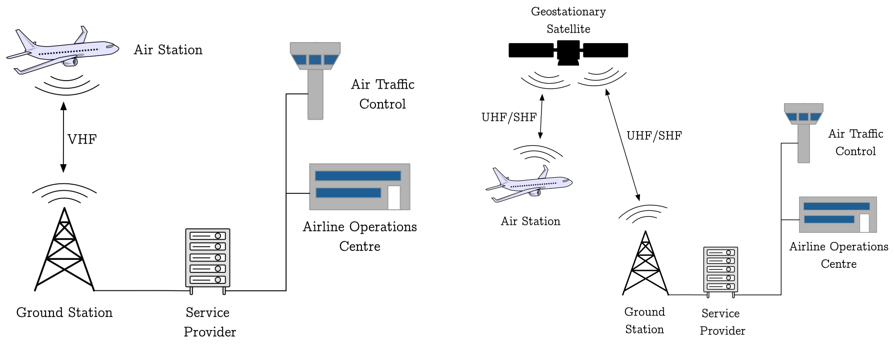
Of particular interest is the 'label' field which allows the Communications Management Unit (CMU) to route ACARS messages to the correct endpoint in the aircraft network [14]. Most labels are standardized in ARINC 620, though

---

[4] Depending on atmospheric conditions, HF frequencies are reassigned regularly.

[5] This depends on the baud rate and keying used.

[6] Exact speeds vary depending on service, here 10 kbps is provided by the Inmarsat ClassicAero service, with the higher rate provided by their SwiftBroadband service.



(a) VHF ACARS infrastructure (b) SATCOM ACARS infrastructure

Fig. 1: High-level diagrams of ACARS modes used in our data collection.

Header Start	Mode	ICAO Reg. or Flight ID	Technical ACK	Label
1	1	7	1	2

Uplink Indicator	Start of Text	Text	Suffix	Block Check Seq. (BCS)	BCS Suffix
1	1	210	1	2	1

(a) Uplink message format

Header Start	Mode	ICAO Reg.	Technical ACK	Label	Downlink Indicator	Start of Text
1	1	7	1	2	1	1

Message No.	Flight ID	Text	Suffix	Block Check Seq. (BCS)	BCS Suffix
4	6	210	1	2	1

(b) Downlink message format

Fig. 2: ACARS message structures for uplink (air-to-ground) and downlink (ground-to-air) based on ARINC 618 [2]. Field sizes in ASCII characters/bytes.

parts of the label space are user defined, including the labels used by the encrypted messages discussed in this paper [3]. The ICAO registration and flight ID fields are useful for identifying the origin of messages. ICAO registrations are unique to an aircraft, allowing identification across flights. In contrast, flight IDs are tied to a single flight and often only used properly by commercial aircraft.

4.3 Uses of ACARS

As mentioned above, ACARS has gradually developed from being used for a narrow set of tasks to being the most general-purpose data link available in aviation. These tasks can broadly be split into two groups — air traffic control and airline operational/administrative messages.

Air traffic control messages are used to ensure that the aircraft can fly on its route safely. This usually takes the form of clearances and informational data. Clearance is needed for an aircraft to fly a particular route, and is organized by ATC. This usually takes place using voice communications, but in congested or remote regions voice channels are difficult to use. ACARS can be used instead, even when voice cannot. Informational data takes the form of reports on relevant flight data such as weather and aerodromes.

Airline operational and administrative messages form a significant part of ACARS traffic. These messages use the free-text nature of ACARS, with messages ranging from automated, structured reporting to text messaging between crew and ground operators. Lists of passengers transferring to other flights, maintenance issues and requests for aid of disabled passengers are common sights, though exact usage varies between airlines. It is also common for flight plans to be served over ACARS, which a pilot will then input into the flight computer.

4.4 Security in ACARS

Although ACARS has no security system mandated or included in its original standard, fully-featured 'add-on' systems are available. These adhere to the ARINC 823 standard, ACARS Message Security (AMS) [4], an example of which is *Secure ACARS*, from Honeywell Inc. [16] — this offers security through a number of common cryptographic algorithms and tools. Outside of this, ARINC are promoting a common implementation in *Protected ACARS* [19]. AMS provides message authentication, integrity and confidentiality protection mechanisms, using modern cryptographic methods. However, implementations are proprietary and subject to little scrutiny beyond internal testing.

Despite the existence of these security suites, deployment is limited. No official statistics exist and since all implementations are proprietary, performing security analysis on them is difficult. In the course of the analysis carried out in this paper, we could not clearly identify any regular use of AMS-based solutions. Furthermore, these systems typically cost extra on top of the standard ACARS service charge which an aircraft operator will pay — this has slowed uptake and created reluctance from the operators to use it. It has also prompted the use and practical deployment of more temporary security solutions, as explored in this paper. To the best of our knowledge, these schemes have no publicly available documentation with regards to implementation.

4.5 Real World Analysis

We utilized three methods of obtaining real-world air traffic data, in line with the capabilities of an honest-but-curious attacker as defined in our threat model. All data collection was done at sites in Continental Europe, with 1,634,106 messages collected in total.

VHF Collection. VHF collection is possible with low investment using the equipment described in Section 3, which can be fed into the ACARSDec decoder.[7] This allows the decoding of 'Plain Old' ACARS signals transmitted around 131 MHz.

---

[7] `https://sourceforge.net/projects/acarsdec/`

Satellite Collection. Collection of L-band SATCOM is similarly achievable with minimal equipment and setup. For example, an L-band (1-2 GHz) horn antenna pointed towards the INMARSAT 3F2 satellite can be fed into band-pass filter and low-noise amplifier. Using an RTL-SDR stick and the open-source JAERO decoder[8] the ACARS message data can be then be recovered. To collect C-band uplink messages more costly antenna would be required.

Third Party Data Sources. In order to compare collected data to a publicly available source, flight tracking websites such as Flightradar24[9] allow verification of many aircraft being in the air or the flights they have completed. However, it is susceptible to government-mandated filtering as explained in in Section 2.1. To get more comprehensive records on aircraft, one can use the Airframes.org database [12]. This provides ICAO registration information and records on aircraft not available on the flight tracker. To the best of our knowledge, this is the most complete and up-to-date publicly available aircraft registration database.

Beyond this, ACARS data has been collected and disseminated on the internet for a number of years. A wide range of ACARS decoders existed in the early 2000s, though most apart from acarsd[10] appear to no longer be maintained. Indeed, the acarsd website lists a range of webservers using the software to produce public ACARS feeds. Some services, such as AvDelphi[11] go further, offering ACARS feeds and tools to understand the messages for a fee.

5 Cryptanalysis of the ACARS Cipher

As our first contribution, we analyze the proprietary cipher used in ACARS communications. Our curiosity was piqued when we noted that some aircraft transmit scrambled ACARS messages, sent primarily with labels '41', '42' and '44' and prefixed by two numbers.[12] In order to decrypt these messages, we follow several classic cryptanalytic steps. We first describe how character substitutions can be recovered before moving to analyze the properties of the cipher.

5.1 Recovering Character Substitutions

Inspecting the available ciphertext, we note that all messages ciphered under this label are prefixed by two digits, from `01` to `09`. We refer to this as the *key identifier*. When messages are grouped by these digits, repeating characters in the same position across messages can be seen. From the similar set of characters used between messages of the same key identifier, this implies the use of a substitution cipher as well as an underlying common structure between messages.

---

[8] `https://github.com/jontio/JAERO`

[9] `https://www.flightradar24.com/`

[10] `http://www.acarsd.org/`

[11] `https://www.avdelphi.com`

[12] Labels '41' and '42' are primarily used in SATCOM and label '44' is most common in VHF — as such we focus our analysis in this way.

Next, frequency analysis can be used to compare the per-character distribution for each key identifier against all messages in our dataset. Since the encrypted messages are a small portion of our overall message set, we expected the character distribution of the underlying plaintext to be similar to the overall ACARS character distribution. Examples of these frequency distributions are shown in Figure 3. We can see two clear peaks, which we match to peaks for frequency analysis per key identifier. This provides a starting point for decryption.

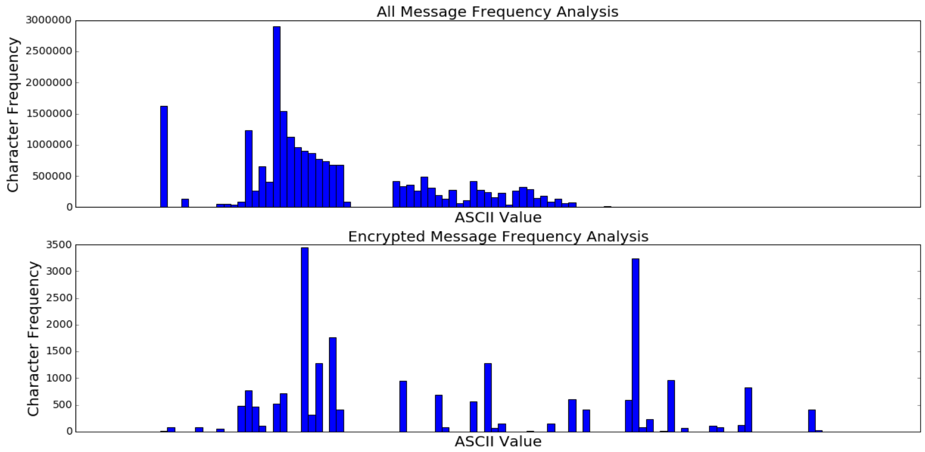


Fig. 3: Character frequency distribution across all received ACARS messages (top) and messages of one key identifier (bottom).

This knowledge can be combined with the fact that some messages sent on the same labels are in plaintext and of similar length. Using the substitutions gained from frequency analysis, we see that the majority of the messages are of a similar structure — later identified as a status update. A labelled plaintext status report message can be seen in Figure 4, in which we identified the fields based on meta-information and structure. Using this, we recover other substituting characters using domain knowledge as explained in the remainder of this section.

5.2 Character Recovery Heuristics

Since we have a limited set of ciphertexts but now possess knowledge about the underlying structure of one message type and content of the fields, we can use heuristics to recover the remaining characters.

Recovering Coordinates. As the second field in plaintext messages is a coordinate field, we use this to retrieve a number of substitution characters exploiting the position of the receiver. Since the reported coordinates are limited to ±2-4 degrees longitude and latitude from a receiver, the options for the first two digits

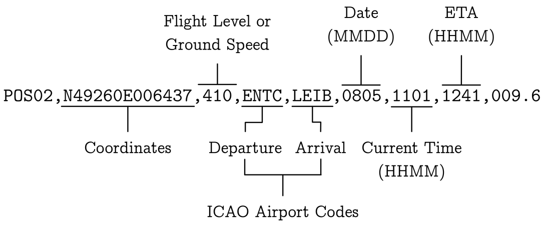


Fig. 4: Plaintext status report message sent under label '44'.

and direction letter (i.e. `N` for north) are restricted. This becomes less reliable if the collection location lies on a point of 0° longitude or latitude.

Message Prefixes. For some message types, the first field follows the structure of a three-letter code followed by two digits which we refer to as a message prefix; in the plaintext example of Fig. 4, this is `POS02`. Looking at all plaintext messages received, one three-letter code is significantly more common. Combined with already known letters, this reveals further substitution characters.

Airport Codes. As indicated in Figure 4, two of the fields are ICAO airport codes. Based again on the collection location, we can determine that local airport codes are more likely and use this as a heuristic for recovering substitutions; for example, if the collection range solely covers a part of the United States, one of the airport codes is likely to begin with `K`. We also exploit partially decrypted messages containing airport codes — which are publicly available — by comparing various possible airport codes with a common encrypted character, revealing many further alphabetic characters.

SATCOM Meteorological Messages. Not all character substitutions can be recovered from the reporting messages as used above. However, aircraft receive periodic meteorological data over the SATCOM uplink to inform the pilots about the weather on their destination airport. Such messages take the form of Pilot Weather Reports (PIREP), Notice to Airmen (NOTAM), Meteorological Aerodrome Reports (METAR) and Terminal Aerodrome Forecasts (TAF). Each has a consistent structure and contains regularly occurring phrases, which allows for character recovery when compared with plaintext obtained from other aircraft.

5.3 Key Recovery

Based on our observations, many of these messages use a limited set of ASCII characters, namely digits `0-9`, characters `A-Z` and symbols `,.*-:/?` and whitespace which falls between the Baudot and limited ASCII sets defined in ARINC 620 [3]. With this in mind, using 2690 messages, from the Baudot set of 44 characters per key we recovered 377/396 (95.2%) of the substitutions across the

Table 2: Number of unique aircraft using the cipher by manufacturer and model. Names have been removed for anonymity.

Manufacturer	**A**			**B**			**C**	**D**	**E**
Model	*A-1*	*A-2*	*A-3*	*B-1*	*B-2*	*B-3*	*C-1*	*D-1*	*E-1*
Avg. Manuf Year	2008	2008	2014	2014	2010	2012	2010	2002	2011
No. per Model	118	56	12	11	3	2	1	1	1
No. per Manuf.	186			16			1	1	1

nine keys. For limited ASCII, with there being 97 substitutions for each key, we recovered 661/873 (75.7%) substitution characters across the nine keys. However, we can decode and read most received messages, implying the Baudot set is closer to the actual character set. By extending the collection range or period, we will be able to recover the remaining characters.

Theoretically, the ACARS alphabet size of 127 offers a potential space of 127! keys. For reasons unknown to us, only 9 of these 3×10^{213} possibilities are used — and they are clearly marked. Furthermore, these keys are shared across all aircraft using this cipher. This significantly reduces the difficulty of recovery by quickly providing sufficient known plaintext for each key.

6 Impact Analysis

Even without recovering every single substitution, the nature of the cipher enables us to still read practically all message content. Indeed, recovering the full keys is a matter-of-time process, simply requiring more messages. This process could be sped up significantly by having many sensors distributed over a wide geographic area, increasing the collection from unique aircraft. In this section, we demonstrate why the weakness of the cipher is a significant problem: the data it should protect is naturally considered private by many of its users.

6.1 Usage Analysis

Our observations indicate that it is exclusively 'business jet' type aircraft that use this encryption. In Table 2 we provide a breakdown of these aircraft by manufacturers alphabetically for anonymity purposes. Manufacturers A and B make up the vast majority of the aircraft transmitting these kinds of messages. In Table 2 we also give a breakdown of models by manufacturer, in which we see that models A-1, A-2, A-3 and B-1 make up the majority of aircraft using this weak cipher. These models are of varying ages, some of which were built within the last two years. On top of this, aircraft appear to either send encrypted messages or not, with no crossover.

In looking for a connection, we found that all models use Primus suite avionics equipment from Honeywell, Inc., pointing towards the source of the cipher. As such, we believe that any aircraft choosing this suite will be affected by the weak cipher, should they opt to use it. Given the use of a small set of global keys, users

Table 3: Absolute and relative distributions of flight tracking website blocks on aircraft transmitting encrypted messages.

Data Set	**Not Blocked**	**Blocked**	**Unknown**	**Total**
VHF	5 (10%)	41 (84%)	3 (6%)	49
SATCOM	10 (6%)	93 (60%)	53 (34%)	156

of many different aircraft models might have the illusion of privacy when in fact this security solution is breakable. Furthermore, we have seen no attempts at key distribution or rekeying over the course of several months; the substitution characters recovered from the first collected data work on our most recent data, too.

6.2 Blocked Aircraft

Although the pool of aviation stakeholders affected is relatively small, the privacy impact is significant simply due to the nature of aircraft using the cipher. This is illustrated by the number of aircraft concealing their existence on flight tracking websites as described in Section 6.2. In Table 3 we see the distribution of ASDI blocks on flight tracking websites for aircraft using this encryption. For ‘not blocked’ aircraft we can see location and flight history, whereas ‘blocked’ are aircraft with some level of ASDI block, i.e. missing flight history or information. We use flight tracking websites for this purpose since they utilize ASDI data; whilst direct ASDI access would be preferable, steps to obtain the feed appear to be outside of the public domain.

We can see that in the VHF set, 90% of the aircraft seen to be using this encryption are making a concerted effort to hide their existence, whereas in the SATCOM set a similar fraction of 94% do the same. This implies that those aircraft are particularly privacy-conscious and using a weak cipher like the one seen here undermines their desire to protect their sensitive information. For example, we observed several ASDI-blocked military-owned jets (United States and Netherlands) using this encryption.

6.3 Security and Privacy Implications of the Message Content

After establishing that the vast majority of encrypting aircraft have a great interest in hiding existence, intent and status of the aircraft, we now consider the content of the encrypted messages and analyze its sensitivity. We collected a total of 2690 messages from encrypting aircraft.

Status Reports. From the 2690 encrypted messages collected, 29.5% are status reports (as seen in Fig. 4). Although we have no official documentation on these messages, from the message format we can deduce with certainty the fields for coordinates, ICAO airport codes, date, current time and ETA. Decrypting these messages reveals a significant amount of potentially private data. As indicated above, many of the aircraft which we have observed transmitting status reports are at least subject to ASDI blocks. We observed that 63.3% of aircraft sending this type of message use an ASDI block, with an even higher percentage of all status reporting messages (90.3%) coming from these aircraft. As such, the blocked aircraft we observed made more use of encrypted position reports than visible aircraft and are undermined greatly by their insecurity.

Airport Information. As part of status reporting messages, both the departure and arrival airports are provided. This reveals a great deal of information on routing, particularly for blocked aircraft. Using this section of the message, not only can we determine the existence of an aircraft but also its intention. Across all status reporting messages, we identified 151 airport codes over 50 country codes, using 1569 instances. From these, 12.6% of instances were from the countries in which data was collected. We claim that using this data, a threat actor can learn a significant amount of information about the aircraft from a single message. By using sensors deployed to cover as great an area as possible, this could allow the tracking of target aircraft without having to cover their entire flightpath.

Free Text Messages. As with airport information, free text messages — especially those relating to flight plans — have the potential to reveal a significant amount of information about an aircraft from a single message. Through this, we saw some examples of using the cipher to protect this type of message. We received 555 free-text messages, 184 of which were related to flight plan administration, with 150 of these revealing the departure/arrival airports. In two instances, in searching for flight plans, previous flight plan information seemingly used by that aircraft were also transmitted.

Meteorological Reporting. Meteorological reports (METAR) are encrypted by a smaller section of the aircraft, primarily over satellite ACARS. We observed 1395 encrypted METAR messages from 125 aircraft, all of which came from satellite collection. Of these, 21.6% of aircraft were ASDI blocked. Whilst the scope for privacy sensitive information is limited, METAR, can also reveal arrival airports.

7 Discussion

As protocols are in use for many decades and are surpassed by technical progress and new user requirements, the temptation for quick fixes is great. In aviation, data links evolved to serve applications for which they were not initially intended (e.g., ACARS for ATC [13]) and requirements changed to include confidentiality to enable privacy for its users. Unfortunately, the presently deployed attempt to protect ACARS does not meet these requirements as we have shown.

It is thus critical to take away several lessons from this study. We strongly believe similar cases can be found not only in the wider aviation scenario but in many safety-focused critical infrastructures using legacy communication systems.

1. As the discussed solution has been greatly obscured, we could not obtain the exact time when it was first deployed but the age of the aircraft using it points to the mid-2000s. This in turn means this solution has been in use for at least 10 years without proper independent analysis. Integrating the security community early on could have avoided the deployment of inferior solutions.
2. The described attack serves to illustrate the dangers of attempting to produce cryptosystems without due peer-review or use of well-known secure primitives — indeed in this case, without any reasonable primitives at all. This is especially the case in this situation where the nature of ACARS limits the cryptographic solution due to characterset, message size and bit rate. Indeed, proposals such as Secure ACARS use AES, which is standardized and widely tested [16]. To draw parallels outside of the aviation scenario, WEP encryption suffered a similar fate in that an attempt to devise a security solution was critically impaired simply by misusing cryptographic primitives [5]. However in the case of WEP, the primitives themselves were sound — in the system discussed in this paper, even the primitives were not sound.
3. Developing — and deploying — solutions without such expertise can indeed be harmful. A solution that provides no effective protection has two distinct negative effects: First, it undermines the development and use of better solutions. In the case of ACARS, a demonstrably secure solution based on ACARS Message Security would be standardized and use reasonable primitives, but users who want data link confidentiality have opted exclusively for the discussed cipher be it for cost or marketing reasons. Secondly, it provides its users with a false sense of security. Believing in the hardness of the encryption may lead operators to rely on the confidentiality they seek and potentially even modify their behavior.

Based on these lessons, we recommend that this security solution should not be used further. With little cryptographic knowledge or resources, message content can be recovered in real time. At the very least, manufacturers should discontinue the inclusion of it in future systems. Ideally, it would be patched out or replaced with a more secure option on existing aircraft and avionics. For users relying on this cipher and seeking better protection, we propose that they demand an established solution such as Secure ACARS which is a more complete security suite.

8 Related Work

Contrary to large parts of the aviation community, the military is aware of security issues in ACARS, see, e.g., [17] where the clear-text nature of ACARS is considered an important weakness. Furthermore, [15] demonstrates efforts to manage the lack of security through encryption, highlighting the requirement for privacy in the military context. In both, ACARS defaulting to clear-text drives users to require some measure of security. As shown in our work, this led to a weak cipher being used widely.

The role of ACARS security has occasionally been discussed outside of academic research. In [1], the authors note the challenges of deploying Secure ACARS, as well as its development process with the US military. Elsewhere, [22] claims to use ACARS to upload malware onto a flight management computer. From this we can see that ACARS is used across aviation, and given the claims of exploitation, the case for encryption is strong.

In [18] and [19] issues caused by the lack of security on standard ACARS are discussed. Particularly in the latter, the authors highlight that crews rely on information sent via ACARS, which could have safety implications. In [23], a security solution is presented but it has not seen production or further analysis of its security properties. As demonstrated these steps are crucial for effective, lasting security.

User perceptions are also notable: [20] shows that out of hundreds of pilots, users of general aviation, and air traffic controllers, who were asked about the integrity and authenticity of ACARS, most believed the protocol offered some kind of protection.

9 Legal and Ethical Considerations

Due to the sensitive nature of this work, we have ensured that it has been conducted in a manner which upholds good ethical and legal practice. At the start of the work we obtained ethical approval process to sensitive messages and we followed a responsible disclosure process with Honeywell, Inc. We adhered to all relevant local laws and regulations.

We have further chosen not to name the aircraft manufacturers and models affected, as this could unduly impact the users of the affected aircraft before there is a chance to address the problem. Furthermore, we have outlined the steps taken to break the cipher but decided to omit further details and example messages in order to avoid making such an attack straightforward to replicate. Overall, we believe it is crucial that all aviation users are aware of weak security solutions protecting their communications so that they do not fall prey to a false sense of security but instead can take the necessary steps to protect themselves.

10 Conclusion

In this paper we have demonstrated the shortcomings of a proprietary encryption technique used to protect sensitive information relating to privacy-aware aircraft operators. More specifically, we have shown that it cannot meet any security objective. As such we recommend its users are made fully aware that it does not provide actual protection; thus, users should either seek a more robust security solution or avoid using ACARS for sensitive material.

We demonstrated the privacy issues arising due to this, since the cipher is primarily used to transmit locations and destinations by aviation users attempting to hide their existence and intentions. We show the cipher's weakness consistently undermines the users' efforts to hide their positional reporting, or protect message content which might be valuable to an attacker.

Consequently, we claim that when such solutions are deployed in practice it does more harm than good for users who require confidentiality from their data link. It is crucial that the aviation industry takes the lessons learned from this case study and addresses these problems before they are widely exploited in real-world attacks.

Acknowledgements

This work has been funded by armasuisse under the Cyberspace and Information research program. Matthew Smith has been supported by the Engineering and Physical Sciences Research Council UK (EPSRC UK), as part of the Centre for Doctoral Training for Cyber Security at the University of Oxford. Daniel Moser has been supported by the Zurich Information Security and Privacy Center. It represents the views of the authors.

References

[1] C. Adams. Securing ACARS: Data Link in the Post 9/11 Environment. *Avionics Magazine*:24–26, June 2006.

[2] Aeronautical Radio Inc. (ARINC). 618-7: Air/Ground Character-Oriented Protocol Specification. Technical Standard. 2013.

[3] Aeronautical Radio Inc. (ARINC). 620-8: Datalink Ground System Standard and Interface Specification. Technical Standard. 2014.

[4] Aeronautical Radio Inc. (ARINC). 823-P1: DataLink Security, Part 1 - ACARS Message Security. Technical Standard. 2007.

[5] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. In *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom)*, 2001.

[6] Federal Aviation Administration. Access to Aircraft Situation Display (ASDI) and National Airspace System Status Information (NASSI). 2011. URL: `https://www.federalregister.gov/documents/2011/03/04/2011-4955/access-to-aircraft-situation-display-asdi-and-national-airspace-system-status-information-nassi` (visited on 11/11/2016).

[7] Federal Aviation Administration. Access to Aircraft Situation Display to Industry (ASDI) and National Airspace System Status Information (NASSI) Data. 2012. URL: `https://www.federalregister.gov/documents/2012/05/09/2012-11251/access-to-aircraft-situation-display-to-industry-asdi-and-national-airspace-system-status` (visited on 11/11/2016).

[8] Federal Aviation Administration. Access to Aircraft Situation Display to Industry (ASDI) and National Airspace System Status Information (NASSI) Data. 2013. URL: `https://www.federalregister.gov/documents/2013/08/21/2013-20375/access-to-aircraft-situation-display-to-industry-asdi-and-national-airspace-system-status` (visited on 11/11/2016).

[9] Federal Aviation Administration. Limiting Aircraft Data Displayed via Aircraft Situation Display to Industry (ASDI) (Formerly the Block Aircraft Registration Request (BARR) Program). 2016. URL: `https://www.fly.faa.gov/ASDI/asdi.html` (visited on 11/11/2016).

[10] D. Gloven and D. Voreacos. Dream Insider Informant Led FBI From Galleon to SAC. 2012. URL: `http://www.bloomberg.com/news/articles/2012-12-03/dream-insider-informant-led-fbi-from-galleon-to-sac` (visited on 11/11/2016).

[11] International Civil Aviation Organization. Global Air Navigation Plan Fourth Edition. Tech. rep. Montreal: International Civil Aviation Organization, 2013, pp. 1–20. URL: `http://www.icao.int/publications/Documents/9750_4ed_en.pdf`.

[12] R. D. Kloth. Airframes.org. 2016. URL: `http://www.airframes.org/` (visited on 11/11/2016).

[13] R. T. Oishi and A. Heinke. Air-Ground Communication. In C. R. Spitzer, U. Ferrell, and T. Ferrell, editors, *Digital Avionics Handbook*, pp. 2.1 –2.3. CRC Press, 3rd ed., 2015.

[14] R. T. Oishi and A. Heinke. Data Communications. In C. R. Spitzer, U. Ferrell, and T. Ferrell, editors, *Digital Avionics Handbook*, pp. 2.7 –2.13. CRC Press, 3rd ed., 2015.

[15] C. Risley, J. McMath, and B. Payne. Experimental Encryption of Aircraft Communications Addressing and Reporting System (ACARS) Aeronautical Operational Control (AOC) Messages. In *20th Digital Avionic Systems Conference*. IEEE, Daytona Beach, 2001.

[16] A. Roy. Secure Aircraft Communications Addressing and Reporting System (ACARS). US Patent 6,677,888. Jan. 2004.

[17] A. Roy. Security Strategy for US Air Force to Use Commercial Data Link. In *19th Digital Avionics Systems Conference*. IEEE, Philadephia, 2000.

[18] M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic. On the Security and Privacy of ACARS. In *Integrated Communications Navigation and Surveillance Conference (ICNS)*. Herndon, 2016.

[19] P. E. Storck. Benefits of Commercial Data Link Security. In *Integrated Communications, Navigation and Surveillance Conference (ICNS)*. IEEE, Herndon, 2013.

[20] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic. On Perception and Reality in Wireless Air Traffic Communication Security. *IEEE Transactions on Intelligent Transportation Systems*, 2016.

[21] M. Strohmeier, M. Smith, M. Schäfer, V. Lenders, and I. Martinovic. Assessing the Impact of Aviation Security on Cyber Power. In *8th Interna-*

tional Conference on Cyber Conflict (CyCon). NATO CCD COE, Tallinn, 2016.

[22] H. Teso. Aircraft Hacking: Practical Aero Series. Presented at The Fourth Annual Hack in the Box Security Conference in Europe (HITB). Amsterdam, NL, Apr. 2013.

[23] M. Yue and X. Wu. The Approach of ACARS Data Encryption and Authentication. In *International Conference on Computational Intelligence and Security (CIS)*. IEEE, 2010.