Institution: University of Oxford		
Unit of Assessment: 11 Computer Science and Informatics		
Title of case study: Improving Security and Privacy of Next Generation Aviation Networks		
Period when the underpinning research was undertaken: January 2012 – August 2019		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Ivan Martinovic Martin Strohmeier	Professor of Computer Science Research Officer	Jan 2012 – present Oct 2016 – present
Period when the claimed impact occurred: 2014 – August 2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

Our application of system security analysis to widely deployed avionic systems has revealed a range of security and privacy challenges in technologies on which modern aviation relies. Our work has discovered practical cyber-attacks on modern surveillance systems and systematic leakage of sensitive data by privacy-sensitive aircraft operators. These insights have formed the basis for policy changes by air traffic regulators including the International Civil Aviation Organization, operational improvements by carriers, and new product developments by equipment manufacturers operating worldwide. We have also contributed to the establishment of the OpenSky Network, a worldwide volunteer aviation sensor network dedicated to enabling air-traffic analysis at scale for regulators, industry, and research institutions, which in 2020 provided flight data to the Bank of England for its quarterly Monetary Policy Report studying the economic impact of COVID-19 upon the UK.

2. Underpinning research

Modern Air Traffic Control (ATC) technologies are increasingly reliant on digital communication systems. These underpin aircraft surveillance, collision avoidance, and air-to-ground communications. Digitalisation of aviation technologies is driven by an international modernisation effort led by regulators such as the International Civil Aviation Organization (ICAO), US Federal Aviation Authority (FAA), and the European Organisation for the Safety of Air Navigation (EUROCONTROL); this effort is ongoing and will continue until at least 2035. Research into air-traffic and communications security is undertaken by a team led by Professor Ivan Martinovic in the Department of Computer Science, University of Oxford, in collaboration with partners at Technische Universität, Kaiserslautern, and the Swiss government agency Armasuisse. This work began in 2012, with results published from 2013 onwards. The research output from these activities includes 6 journal articles and 12 conference papers (including best paper award at DASC 2015, an avionics venue). The work has focussed on four topics: (1) security in next generation air traffic surveillance (e.g., the ADS-B protocol); (2) privacy leakage from wireless air-to-ground data links (e.g., the ACARS protocol); (3) identification of encryption vulnerability used in aviation equipment manufactured by Honeywell; and (4) the open-access crowdsourcing network run by volunteers, OpenSky, which monitors over 98% of all European air traffic in real time.

(1) Active attacks against Automatic Dependant Surveillance – Broadcast (ADS-B) [R1, R3, R4].

ADS-B provides cheaper aircraft surveillance over a wider area – it is a key enabler for future air traffic control and its presence is mandated on aircraft by 2025. Research in [**R1**] shows that message injection, modification, and deletion attacks on ADS-B are not only possible but inexpensive. We extended this work with a real-world feasibility analysis which concluded that safety-critical air traffic decision processes should not exclusively rely on the ADS-B system [**R3**]. Our work in [**R4**] used this research as a basis to assess the aviation industry perception of the security of systems such as ADS-B, identifying that, in many cases, industry professionals felt that aviation systems had security mechanisms where none in fact existed.

(2) Aviation data link private data leakage [R6].

Within [**R6**] we conducted a measurement study to assess sensitive information leakage on a widely used aviation data link, the Aircraft Communications Addressing and Reporting System (ACARS). We identified that the use of ACARS by business, government, and military aircraft consistently undermines their efforts to obscure their movements from observation, by revealing flight details they otherwise seek to keep private. Commercial aircraft are also shown to transfer sensitive passenger details including names, onward destinations, and, in some cases, medical information or full credit card details transferred in the clear.

(3) Usage of weak encryption on data links [R5].

Extending topic (2), research presented in [**R5**] revealed that a cipher used by many non-commercial aircraft to provide confidentiality on the Aircraft Communications Addressing and Reporting System (ACARS) can be readily broken. We assess the impact on privacy and security for its unsuspecting users by characterizing months of real-world data, decrypted by breaking the cipher and recovering the keys. In turn, [**R5**] shows that the decrypted data leaks private and sensitive information including the existence, intent, and status of aircraft owners who otherwise attempt to protect their privacy, supporting our findings in [**R6**]. This vulnerability has been reported (following the responsible disclosure process) to the manufacturer, Honeywell.

(4) Development of Crowdsourced Sensor Network [R2].

We co-founded the OpenSky Network crowdsourced sensor network as described in [**R2**], established with the aim of collecting aviation surveillance signals worldwide for research purposes. The platform gathers messages and physical layer information sent by aircraft and drones, such as Mode S and ADS-B data, and makes it available for further analysis using scalable and efficient processing architecture. Since launch, OpenSky has grown into the largest aviation research platform worldwide, and currently (July 2020) processes around 280,000 messages per second; it covers 190 countries with over 2,000 sensors installed by volunteers. This has been leveraged in our work, including [**R5**] and [**R6**], where we used the data to identify aircraft concealing their movements.

3. References to the research

[**R1**] M. Schäfer, V. Lenders, I. Martinovic: Experimental Analysis of Attacks on Next Generation Air Traffic Communication**.** 11th Int. Conf. on Applied Crypto. and Network Security (ACNS), 2013: https://doi.org/10.1007/978-3-642-38980-1_16.

[**R2**] M. Strohmeier, M. Schäfer, M. Fuchs, V. Lenders, I. Martinovic: OpenSky: A Swiss Army Knife for Air Traffic Security Research. IEEE/AIAA 34th Digital Avionics Systems Conf. (DASC), 2015: https://doi.org/10.1109/DASC.2015.7311411. *Best Paper Award*.

[**R3**] M. Strohmeier, V. Lenders, I. Martinovic: On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. IEEE Comms Surveys & Tutorials, 2015: https://doi.org/10.1109/COMST.2014.2365951. In [**E6**], as “Strohmeier 2013” (arXiv pre-print).

[**R4**] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, I. Martinovic: On Perception and Reality in Wireless Air Traffic Communication Security. IEEE Tr. on Intelligent Transportation Systems, 2017: https://doi.org/10.1109/TITS.2016.2612584.

[**R5**] M. Smith, D. Moser, M. Strohmeier, V. Lenders, I. Martinovic: Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS. Int. Conf.on Financial Crypto. and Data Sec., 2017: https://doi.org/10.1007/978-3-319-70972-7_15.

[**R6**] M. Strohmeier, M. Schäfer, M. Fuchs, I. Martinovic, V. Lenders: Undermining Privacy in the Aircraft Communications Addressing and Reporting System (ACARS). 18th Privacy Enhancing Tech. Symp. (PETS), 2018: https://content.sciendo.com/configurable/contentpage/journals$002fpopets$002f2018$002f3$002farticle-p105.xml

4. Details of the impact

Ongoing aviation modernisation efforts are focussing on improving efficiency and safety whilst lowering costs. Fundamental to this change is having more detailed data streams: this includes protocols used in ATC (Air Traffic Control)-related operations such as aircraft surveillance and collision avoidance, but also protocols used for general data-link communication between aircraft and ground stations, and carrying information such as the medical status of passengers and payment details for in-flight transactions.

Most of these systems were designed decades ago, and lack resilience against malicious actors under well-accepted modern threat models. The main reason for this is that ATC has long focussed on safety, i.e., making systems resilient to faults that occur naturally and unintentionally. This 'historical mindset' ignores intentional malicious behaviour, which is at the centre of security research. Our impact stems from our demonstration of the scope for malicious activity – providing the evidence base for policy changes throughout the industry. Concretely, our work has led to the following:

1. Impact on regulatory policy and commercial operations
2. Impact on national-level procurement
3. Open provision of aircraft data

Impact on Regulatory Policy and Commercial Operations.

At the international level, the International Civil Aviation Organization (ICAO) has recognised for the first time the need to validate ADS-B-derived information [**E1**]. Our work is cited as evidence that ADS-B data cannot be solely relied upon for ATC, and so that a proposed full transition away from secondary transponder radar or multilateration systems cannot take place without new security measures.

At the level of national governance, our work is cited in policy documents or directly confirmed by government agencies in multiple countries. In 2016 the United States Department of Defense (DOD) issued a Call for Proposals for research towards securing ADS-B [**E2**], referencing our work [**R3**] as principal motivation. The call's objective was to "develop a modular, secure, and affordable solution for Automatic Dependent Surveillance Broadcast (ADS-B) for Air Force platforms". It uses our research as the primary evidence for the need to mitigate the lack of security in ADS-B: "while ADS-B will play an essential role in the future of air traffic control, the inherent lack of security measures in the ADS-B protocol is a reason for concern. The problem has recently been widely reported in the press and at hacker conventions. Academic researchers, too, proved the ease of compromising the security of ADS-B with current off-the-shelf hard- and software (Ref 2). It has also been estimated that it will cost billions of dollars to retrofit all DoD aircraft with ADS-B technology. Given these numbers and the looming ADS-B Out FY 2020 mandate, it is readily apparent that there is a need for a practical, secure and affordable solution to transitioning NextGen technology into the DoD/civilian fleet of aircraft."

"(Ref 2)" refers to the preprint version of our paper [**R3**] and in turn elements of [**R1**] where the experimental analysis of active attacks on ADS-B was first conducted.

More recently, the United States Government Accountability Office issued a report to congressional committees in January 2018 on the "Urgent Need for DOD and FAA to Address Risks and Improve Planning for Technology That Tracks Military Aircraft" [**E3**], again citing our work in [**R3**]. In Switzerland, meanwhile, "based on the recent research insights regarding the insecurity of many civil and military aircraft communication systems" articulated in [**R1-R6**], the government “has invested significant funds to build a new avionics laboratory in its headquarters in Thun” as “a priority undertaking”, and the Swiss Air Force “has decided to make a distinction between traditional electronic warfare threats and new cyber security threats to aircraft” [**E4**]. Our work has further been incorporated in assessments of cyber-security for critical national infrastructure by the governments of Singapore [**E5**] and Sweden [**E6**], citing our work on ADS-B, and the Netherlands [**E7**] (citing [**R1-R3**]).

Indeed, our work has promoted awareness of cyber-security issues across the entire aviation community, from individual pilots [**E8**] to airlines [**E9**] – underpinning pressure on air traffic regulators to address the insecurity issues in aircraft data links. Swiss Air undertook system improvements to mitigate a vulnerability we discovered [**R5**] and responsibly disclosed to them [**E9**], in which passenger credit card details were broadcast without encryption whenever an onboard payment was made. Our work thereby benefitted not only Swiss Air from a data-protection perspective, but also any of the more than 16,000,000 passengers carried by the airline annually who have made onboard purchases since the system improvement.

Impact on National-level Procurement.

Armasuisse is the Federal Office for Defence Procurement within the Swiss Confederation. It is the sole procurement organisation for defence and civil protection purposes in Switzerland. They confirm in their letter [**E4**] that our aviation security research has changed their procurement process in two major ways. Firstly, introducing the requirement for systems to provide physical-layer data to enable detection and mitigation of attacks on ATC communication links (based on our work [**R1-R6**]). Secondly, requiring the inclusion of cyber-security testing in the procurement of national ATC surveillance systems. This testing particularly considers the fake message injection attacks identified in our work [**R3**]. This second activity is already occurring in practice, with Armasuisse writing in [**E4**]: “we have used approaches, knowledge, and software developed in collaboration with Oxford to conduct extensive in-the-field penetration testing of the new Multilateration system currently procured by the Swiss air traffic control company Skyguide”.

Open Provision of Aircraft Data.

The OpenSky Network operates over 2,000 sensors worldwide and serves approximately 3,000 members, including national air traffic regulators and EUROCONTROL (the Europe-wide air traffic body). The value of this open data is keenly recognised in the air-traffic sector. EUROCONTROL’s Performance Review Unit is incorporating feeds from the OpenSky Network into their activities in “monitoring and reviewing the performance of the pan-European air navigation services (ANS) system”, as part of a broader mission to coordinate and harmonise air-traffic management across Europe [**E10**]. The unit notes that with the incorporation of the OpenSky Network as a source “[t]he additional data will enhance the tracking of aircraft movement, particularly in terms of better accuracy, higher reporting rate and faster access to data” [**E10**].

The importance of open data has come rapidly into focus with the emergence of the COVID-19 pandemic. In an April 2020 publication [**E11**], the International Monetary Fund (IMF) recommended the data provided by the OpenSky Network as a source for use in measuring an economy’s external sector (that country’s economic relationships with the rest of the world) when faced with emergency circumstances. Further, in May 2020, the OpenSky Network provided flight data to the Bank of England for the preparation of its quarterly Monetary Policy Report [**E12**], which studied the economic impact of COVID-19 upon the UK. The data were used to highlight the sharp decline in the number of aircraft departures, both in the UK and worldwide. Data from the OpenSky Network is also referred to as a high-frequency indicator for gross domestic product (GDP) forecasting. The report states: “as business output surveys are providing a less useful steer than usual, Bank staff are using a wider range of indicators to gauge how GDP is likely to evolve”. Four data sources were highlighted as such high-frequency indicators, with the OpenSky Network the sole resource for flight traffic levels. This was contributory to the bank’s estimate that “monthly GDP will fall by enough in March to pull GDP down by around three percent" [**E12**.1]. Use of OpenSky data continued in the following quarterly Monetary Policy (August 2020) [**E12**.2].

In addition to the impacts on regulatory policy, commercial flight operations, and defence procurement arising from our work on the security of aircraft communications systems, the open provision of aircraft data through OpenSky has given rise to further impacts on national-level data policy and on systems development in industry. The development of OpenSky in collaboration with Armasuisse was itself a technical case study in big-data management for security and defence purposes [**E4**]. Beyond uses in government and policymaking, OpenSky Network data is also integrated into more than 20 open projects including the LiveTraffic module for the commercial-grade and FAA-certifiable flight simulator X-Plane. (It is also included as core functionality in the free GeoFS flight simulator.) [**E13**]. In industry, companies manufacturing ATC monitoring systems now provide interoperability with the OpenSky Network: for example, Günter Köllner Embedded Development GmbH (trading as jetvision), which produces and markets receivers specifically for the OpenSky Network [**E14**]; and SeRo Systems GmbH, which also provides high-end sensors that are interoperable with OpenSky, and used for collection and processing of Mode S and ADS-B data for aviation traffic management [**E15**].

5. Sources to corroborate the impact

[**E1**] ICAO Technical Commission Working Paper, Document A39-WP/296, at para. 2.6: http://www.icao.int/Meetings/a39/Documents/WP/wp_296_en.pdf.
[**E2**] US Department of Defence (2015): Call for Proposals for Modular, Secure and Affordable Design for NextGen ADS-B Integration: https://www.sbir.gov/sbirsearch/detail/870253.
[**E3**] US GAO Report to Congressional Committees, GAO-18-177, Jan 2018, at pp. 15-16: https://www.gao.gov/assets/690/689478.pdf.
[**E4**] Letter from Armasuisse Science and Technology Director detailing the impact of the Oxford research on policy and procurement, September 2020.
[**E5**] Civil Aviation Authority of Singapore paper on Aviation Security: CAAS J. of Aviation Management, 2014, at pp. 73-84: https://saa.caas.gov.sg/journal-of-aviation-management.
[**E6**] Swedish Defence Research Agency Report, December 2013, at p. 10.
[**E7**] Netherlands Annual Review of Military Studies, 2016, at pp. 309-23: http://www.springer.com/la/book/9789462651340.
[**E8**] Industry magazine article reporting the research: InterPilot March 2014, "Who controls your aircraft?", at p. 24: https://www.beca.be/com-docman/safety/39-aviation-magazines/ifalpa-interpilot-magazine/99-ifalpa-interpilot-magazine.html.
[**E9**] Evidence from responsible disclosure process with Swiss International Air Lines Ltd. and Lufthansa Technik AG.
[**E10**] Supporting Statement from EUROCONTROL Performance Review Unit regarding the impact of OpenSky data on pan-European air traffic monitoring, March 2020.
[**E11**] IMF Report, "Ensuring Continuity in the Production of External Sector Statistics During the COVID-19 Lockdown", April 2020, at p. 10: https://www.imf.org/en/Publications.
[**E12**] Bank of England, Monetary Policy Reports. (1) May 2020, at pp. 22, 34: https://www.bankofengland.co.uk/report/2020/monetary-policy-report-financial-stability-report-may-2020; (2) Aug 2020, at p. 26: https://www.bankofengland.co.uk/report/2020/monetary-policy-report-financial-stability-report-august-2020.
[**E13**] Use of OpenSky data in commercial-grade flight simulator X-Plane (https://twinfan.gitbook.io/livetraffic/) and open flight simulator GeoFS (https://www.geo-fs.com/pages/credits.php).
[**E14**] OpenSky Network Kit produced by jetvision: https://archive.vn/7QcNI.
[**E15**] Letter from Managing Director, Sero Systems, regarding impact of OpenSky Network data on the company's products.